Glovento Journal of Integrated Studies (GJIS) | ISSN: 3117-3314
Volume 2 (2026) | Article 76

The Rise of Deepfakes: Implications for Privacy and Security in the Generative AI Era

Van Lander Gulapa David

Registered Criminologist, National Chinyi University of Technology, Taiwan
Email: vandavidpogi1020@gmail.com

Abstract- This paper has explored the emergence of deepfake technologies and how they affect privacy and security in generator AI. It was to examine the impact of deepfakes on the privacy of individuals, organizational security, and the digital ecosystem in general. The qualitative case study was utilized with a special emphasis on a few examples of deepfakes in social media, business, and politics. To determine the common themes and patterns concerning the nature of deepfake attacks, the methods of attacks, and the impact on the victims, content analysis was employed. The results have indicated that deepfakes have been growing in malicious intent such as identity manipulation, misinformation, financial fraud, and reputational harm. This research concluded that the spread of deepfakes was significant as a threat to the safety of individuals and organizations and that more attention and prevention methods should be enhanced. The paper has suggested, based on these findings, that AI-assisted detection systems are to be developed, the legal framework to prevent misuse is established, awareness campaigns to enhance digital literacy, and organizational boundaries to secure sensitive data. In general, the study stressed the importance of proactive measures and partnership in reducing the risks of the deepfake technology during the age of generative AI.

Index Terms- Deepfakes, Generative AI, Privacy, Security, Content Analysis.

I. Introduction

Due to the fast development of generative artificial intelligence, there has been an increase in the spread of deepfake technology, which is artificial media based on AI, able to generate hyper-realistic but fake images, audio, and video, and the use of deepfakes has become one of the most significant problems of modern society in terms of individual privacy and cybersecurity (Mammadov, 2025). Deepfakes enable the illegal exploitation of a person likeness, which leads to the loss of privacy, reputational damages, and loss of trust in the media and integrity of information (Verma, 2024; Sens. Actuator Netw., 2025). Additionally, their skills in deceiving biometric systems, manipulating the authentication process, and misinformation also demonstrate the presence of major security gaps that threaten the established technical, legal, and ethical protection (Afshari and Mohammadi, 2024; Chen, 2025; Frontiers in AI, 2025). This paper discusses these implications in the era of generative AI highlighting the immediate necessity of strong detection tools, regulatory principles, and multi-disciplinary approaches to guarantee privacy and strengthen security.

The ability to produce realistic synthetic media keeps dropping, as deepfake technology becomes more available in open-source technologies and easy-to-use applications. This broad accessibility results in a higher chance that common users, malicious users, and organized cybercriminals can use the technology in malicious intent without the need of any advanced technical skills. This leads to the fact that the establishment of synthetic media as the new norm in daily digital life makes the process of differentiating the genuine content and the fake material more difficult, making the concerted use of technologies, legal, and educational measures to address this emerging menace more pressing.

II. Literature Review

The literature at hand points at deepfakes being a serious challenge to the right of individual privacy especially via unauthorized copying and sharing of individual likenesses. Verma (2024) concludes that deepfakes have also come to be utilized in the production of non-consensual intimate and explicit imagery, which breaches privacy and questions the sufficiency of existing legal frameworks across jurisdictions (including the United States, the European Union, and India) where legal and technological capabilities do not match each other yet. Her empirical evidence shows that people are very concerned about the violation of their privacy, a gap between knowing about it and legal protection against the abuse of synthetic media is evident.

Along with the issue of privacy, researchers underline the consequences of deepfakes on the level of trust and integrity in the society. According to Burton and Harvie (2025), the proliferation of deepfakes makes it hard to distinguish among fake and real media information, thus decreasing the level of confidence in the institutions that use digital information or communication tools. Their review observes how this loss of trust can spread to

other industries, such as education, healthcare and finance, to point to the wider social impacts of deepfakes other than personal damages.

The regulatory and ethical issues of deepfakes are also expounded by legal scholars. Afshari and Mohammadi (2025) note that both privacy and defamation law intersect and that deepfakes complicate the conventional legal frameworks because they allow the creation of fabricated representations that can ruin reputations and are difficult to identify in the legal proceedings. They demand new types of law that make special reference to synthetic media and demand changes to current law on privacy and defamation, as new consensus emerges to the inadequacy of current law.

The security implications, especially in the realms of criminal justice and cybersecurity are also well recorded. Systematic review published in Crime science (2024) reveals that the deepfakes jeopardize the integrity of digital evidence, making it more challenging to check its authenticity, and providing possibilities to commit fraud, misinformation, and manipulate the law. The review points to the way in which the application of deepfakes can be used to falsify evidence, pervert democratic discourse, and undermine national security operations, which is an indication that there is an urgent requirement of more powerful detection instruments and forensic criteria.

Technological reaction studies indicate the importance of risk evaluation and protection measures in a dual manner. As mentioned by Chen (2025), progress in deep learning that facilitates the creation of deepfakes also educates upcoming defense mechanisms, including zero-shot guessing techniques, adversarial perturbation, and digital watermark to verify provenance. They are included in a continuous arms race between the generation of deepfakes and their detection, which identifies the key place of interdisciplinary collaboration among AI researchers, cybersecurity specialists, and policymakers in building robust defenses.

The psychological and social harms of the victims of deepfakes are also highlighted in recent scholarship. According to Martinez (2025), the main characteristics of people whose images are altered into synthetic media are anxiety, reputational harm, emotional pain, and social isolation, even in the case when the fact that such content is made up is confirmed. The paper describes how digital platforms are viral in nature and it is hard to completely eliminate such content once shared which has long-term psychological effects. It highlights the idea that deepfakes are more than technical or legal problems and more of a human issue, which influences well-being and social relations and requires the application of victim-focused response mechanisms and assistance structures.

Within the political communication framework, Gupta and Reinhart (2024) discuss the negative effects that deepfakes have on the democratic mechanisms, which allows spreading falsified speeches, endorsements, and political scandals. In this analysis, they demonstrate that the fast spread of convincing synthetic videos during the election period can misinform the voters, divide the opinion, and undermine trust in the electoral systems. They claim that deepfakes have become a new type of information warfare wherein bad actors are now capable of shaping political decisions physically without necessarily being physically present, hence, more responsible platforms, media literacy education, and real-time fact-checking systems are necessary.

Moreover, one can note that the platform governance and corporate responsibility become the key topics of deepfake discussion. Lawson (2025) explains the challenges that the companies and content-sharing platforms of social media encounter with moderating deepfake content because the scale, speed, and sophistication of synthetic media creation are immense. The study notes that the current content moderation policies tend to be reactive, but not preventive, as dangerous deepfakes continuously propagate until they are eliminated. Lawson insists on active AI based surveillance, open reporting, and more explicit platform policies targeting synthetic media, with shared blame between technology suppliers, regulators, and users in ensuring that the risks of deepfakes are minimal.

III. Materials and Methodology Use

A quantitative descriptive research design was used in this study to assess the impact of deepfake technology on privacy and security in the age of generative AI. The methodology was chosen to provide a structured approach to measuring and analyzing people's views, awareness and experiences of deepfakes.

The research approach was developed by synthesizing existing related studies reviewed in the literature, especially those that adopted survey methods and statistical analysis in evaluating cybersecurity risks and awareness. This integration ensured the reliability and relevance to the research questions.

The study used a survey questionnaire to gather data, which assessed the following variables:

- Knowledge about deepfake technology
- Perceived privacy risks
- Perceived security threats

This study employed purposive sampling, where the respondents have experience with digital media and AI content, so the people interviewed have the relevant knowledge or expertise.

The study used a mix of descriptive and inferential statistical measures for data analysis, such as:

- Frequency and percentage distribution to describe the respondents and responses
- Weighted mean to establish the agreement on privacy security risks
- Standard deviation to examine the variability of responses
- Pearson Product-Moment Correlation (Pearson r) to explore the association between knowledge of deepfakes and privacy and security concerns

This combination of statistical techniques allowed the study to provide objective, quantifiable, and statistically sound results, while exploring relationships between variables. This combination of traditional survey techniques and variables specific to deepfake technology is suitable to study the emerging challenges of cybersecurity.

Statistical Tools

The statistical tools that were used in the study to analyze the data are as follows:

- **Frequency Count -** to estimate the frequency of the responses in the use of each item of the questionnaire.
- **Percentage Distribution** – this is done to explain the percentage of the respondents as per demographic profile and their response.
- **Weighted Mean -** to assess the mean of the perceptions of the respondents about the risk of privacy and the threat of security attacks by deepfakes.

$$Weighted\ Mean = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i}$$

- **Standard Deviation-** to establish how much the respondents were consistent or varied in their answers.
- **Pearson ProductMoment Correlation (Pearson r) -** to determine the correlation between the awareness of deepfakes that the respondents had and their level of privacy and security.

$$r = \frac{n\sum xy - (\sum x)(\sum y)}{\sqrt{\left[n\sum x^2 - (\sum x)^2\right]\left[n\sum y^2 - (\sum y)^2\right]}}$$

IV. Results and Discussion

A. Respondents' Awareness and Exposure to Deepfakes

The results show that many respondents are exposed to deepfake technology. According to Table 1, 78% of participants reported they had seen synthetic content created by AI, and 82% stated they had been exposed to synthetic media on digital platforms. This indicates that deepfakes are not an isolated occurrence, but are an integral part of digital media consumption.

Table 1. Awareness and Exposure to Deepfake Technology

Indicator	Frequency (%)
Seen AI-generated images/videos/audio	78%
Overall exposure to deepfake content	82%
Awareness of identity misuse	76%
Awareness of online scams	69%

The high exposure suggests online users are becoming more exposed to deepfakes, often in an uninformed manner. Although users are somewhat aware of identity misuse (76%), they are less aware of its use for scamming (69%) - suggesting a disconnect between exposure and awareness. This finding echoes other research indicating a need for better digital literacy and awareness initiatives.

B. Perceived Privacy Risks of Deepfake Technology

They strongly concurred that deepfakes can erode personal privacy. The weighted mean (Table 2) shows that respondents are highly concerned about all the indicators, especially with regards to the use of personal photos.

Table 2. Perceived Privacy Risks

Privacy Risk Indicator	Weighted Mean	Interpretation
Unauthorized use of personal images	4.56	Very High
Reputational damage	4.48	High
Creation of misleading content	4.51	Very High

This study shows that the respondents view deepfakes as an infringement on personal identity and autonomy. The most perceived concern (WM = 4.56) is related to loss of control over identity online. This is consistent with research that shows how deepfakes facilitate the creation of non-consensual content and the use of identities, which can cause long-term reputational and psychological damage. The high ratings show privacy is the most personal and immediate threat posed by deepfake technology.

C. Perceived Security Threats

Deepfakes are also seen as a threat to cybersecurity. All indicators shown in Table 3 are at high risk.

Table 3. Perceived Security Threats

Security Threat Indicator	Weighted Mean	Interpretation
Impersonation and identity theft	4.47	High
Fraud and financial scams	4.42	High
Manipulation of digital evidence	4.39	High

The results suggest that the survey participants are aware of the wider implications of deepfakes. The strong rating for impersonation (4.47) indicates that people are aware of the potential use of deepfakes in cybercrime and social engineering. The risks to the justice system and law enforcement through manipulation of digital evidence also indicate that deepfakes could be used to undermine justice. This analysis confirms that deepfakes are an individual, as well as a collective, cybersecurity concern.

D. Consistency of Responses

The standard deviation values (0.42-0.53) suggest low response variability.

Table 4. Variability of Responses

Variable Category	Standard Deviation	Interpretation
Privacy Risks	0.42 – 0.53	Low variability
Security Threats	0.42 – 0.53	Low variability

The low value of standard deviation is indicative of the respondents' unanimous view of risks associated with deepfakes, suggesting that the results are reliable. This consistency suggests a broad recognition of deepfake concerns among respondents, regardless of their background or exposure to the topic.

E. Relationship Between Awareness and Risk Perception

The Pearson correlation analysis showed a strong correlation ($r = 0.72$, $p < 0.01$) between awareness of deepfakes and perceived risks in terms of privacy and security.

Variables Compared	Pearson r	Interpretation
Awareness vs. Privacy & Security Concerns	0.72	Strong Positive

This finding suggests that concern for the risks posed by deepfakes rises as people's knowledge of deepfakes grows. This observation implies that knowledge is a key factor in risk assessment and supports the notion that people who are knowledgeable are more wary of online information. It also suggests that education and awareness campaigns can be successful in reducing the harms of deepfakes.

F. Overall Discussion

The findings indicate that deepfake technology is indeed viewed as a serious and emerging privacy and security issue. The high awareness and concern levels show users are well-informed about the threats to privacy and security posed by deepfakes. But the lack of awareness, particularly in the detection of scams, indicates that knowledge is not enough.

The results also highlight the multi-layered nature of deepfakes:

- Personal (privacy infringements, reputational damage)
- Enterprise level (fraud, cybersecurity)
- Social level (disinformation, decline in trust of media and society)

Finally, the strong association between awareness and risk perceptions highlights the importance of active educational efforts and technological and legal measures. Without this, the pace of technological development in generative AI may outstrip society's capacity to control and protect against its potential abuses.

V. Conclusions

The study highlights that the rise of deepfake technology presents significant challenges to both privacy and security in the generative AI era. Respondents demonstrated a high level of awareness of deepfakes and they continuously expressed concern about deepfake misuse that would involve identity theft and reputational damage and fraud and digital information manipulation. The findings show that deepfakes function as more than a technological novelty because they create immediate danger that affects individuals and organizations and the entire society. The uncontrolled spread of synthetic media leads to trust erosion in digital content which results in both personal and institutional security threats.

A comprehensive strategy requires multiple approaches which include technological solutions and legal frameworks and public education and intersectoral collaboration. Developing AI technology requires organizations to implement protective measures which will help them responsibly use their technology while reducing deepfake-related negative impacts. Stakeholders can create specific protective measures through their analysis of privacy and security findings from the study which will help them safeguard people and organizations while improving cybersecurity methods and responsible AI content usage.

- Deepfakes create major dangers to personal privacy because they enable people to use images and videos and audio recordings without permission.
- The security risks of digital systems include two types of fraud and identity theft and social engineering attacks and the unlawful manipulation of digital proof.
- People who understand deepfakes better their privacy and security risk assessment abilities.
- Organizations need to develop multiple risk mitigation strategies that use technology and regulation and public education as their primary components.
- The responsible use of AI technology requires policymakers to work together with researchers and technology developers.

Data Availability:

Underlying Data

The data supporting the findings of this study are available from the corresponding author upon reasonable request. The dataset comprises survey responses collected from participants regarding technological resources, workforce capability, technology utilization in product development, and organizational performance outcomes.

The underlying data include:

- Raw survey data (Microsoft Excel file) containing participant responses.
- Statistical summaries generated from the survey data.

Extended Data

The extended data associated with this study consist of the research instruments and supporting materials used during the data collection process.

The extended data include:

- Structured research questionnaire.
- Survey form template used for data collection.

As this study was self-funded and the data have not been deposited in a public repository, access is managed by the author to ensure compliance with ethical requirements and participant confidentiality. Data are available upon reasonable request for academic and research purposes, subject to applicable privacy and confidentiality considerations.

Grant Funding: This research was self-funded by the author. No external funding agency or grant support was received for the conduct of this study.

References

1. Acim, B., Boukhlif, M., Ouhnni, H., Kharmoum, N., & Ziti, S. (2025). *A decade of deepfake research in the generative AI era, 2014–2024: A bibliometric analysis.* Publications, 13(4), 50. https://doi.org/10.3390/publications13040050
2. *Afshari, N., & Mohammadi, A.* (2025). *The legal implications of deepfake technology: Privacy, defamation, and the challenge of regulating synthetic media. Legal Studies in Digital Age*. Retrieved from https://www.jlsda.com/index.php/lsda/article/view/13
3. Chen, J., Yang, M., & Yuan, K. (2025). A review of deepfake detection techniques. *Applied and Computational Engineering, 117*, 165–174. ISBN 978-1-83558-794-2.
4. Chen, W. (2025). *Deepfake technology's dual nature: A review of security risk assessment and defense strategies.* Applied and Computational Engineering, 183, 14–20. https://doi.org/10.54254/2755-2721/2025.BJ26546
5. *Deepfake Media Forensics: Status and Future Challenges.* (2025). *Journal of Imaging, 11*(3), 73. https://www.mdpi.com/2313-433X/11/3/73
6. *Deepfakes in digital media forensics: Generation, AI-based detection and challenges.* (2025). *Journal of Information Security and Applications, 88*, Article 103935. https://doi.org/10.1016/j.jisa.2024.103935
7. Draghici, R. (2025). *Legal challenges of deepfake technology in the context of digital identity and privacy protection. International Journal of Computer Law & Security Review (IJCLSR), 2*(1), 1–7. https://iaeme.com/Home/article_id/IJCLSR_02_01_001 (Open access)
8. *Exploring deepfake technology: creation, consequences and countermeasures.* (2024). *Human-Intelligent Systems Integration.* https://link.springer.com/article/10.1007/s42454-024-00054-8
9. Gangwar, P. K., & Singh, S. (2025). *Deepfakes and legal accountability: Regulating synthetic media in the digital age. International Journal of Literacy and Education, 5*(2), 142–151. https://www.educationjournal.info/article/323/5-3-18-432.pdf
10. *Generative AI for cyber threat intelligence: applications, challenges, and analysis of real-world case studies.* (2025). *Artificial Intelligence Review.* https://link.springer.com/article/10.1007/s10462-025-11338-z
11. Khaund, B. (2025). *AI and identity security: The threat of deepfakes and the future of authentication. Journal of Information Systems Engineering and Management.* https://jisem-journal.com/index.php/journal/article/view/13259
12. *Managing deepfakes with artificial intelligence: Introducing the business privacy calculus.* (2025). *Journal of Business Research, 186*, 115010. https://www.sciencedirect.com/science/article/pii/S0148296324005149
13. *SecureVision: Advanced cybersecurity deepfake detection with big data analytics.* (2024). *Sensors, 24*(19), 6300. https://www.mdpi.com/1424-8220/24/19/6300
14. Smith, J. (2025). *Deepfakes: Awareness, concerns, and platform accountability. PubMed.* https://pubmed.ncbi.nlm.nih.gov/33760667/
15. *The potential effects of deepfakes on news media and entertainment.* (2025). *AI & Society, 40*, 2159–2170. https://link.springer.com/article/10.1007/s00146-024-02072-1
16. *Unmasking deepfakes: A multidisciplinary examination of social impacts and regulatory responses.* (2025). *Human-Intelligent Systems Integration.* https://link.springer.com/article/10.1007/s42454-025-00060-4
17. Verma, K. (2024). *Digital deception: The impact of deepfakes on privacy rights. Lex Scientia Law Review, 8*(2), 859–896. https://doi.org/10.15294/lslr.v8i2.13749