International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I4P106

Volume 72 Issue 4, 51-57, April 2024


*Short Communication*

# Generative AI Security: Protecting Users from Impersonation and Privacy Breaches

Saurav Bhattacharya[1], Suresh Dodda[2], Anirudh Khanna[3], Sriram Panyam[4], Anandaganesh Balakrishnan[5], Mayank Jindal[6]

[1]*InfoSec Expert, Microsoft, Seattle, WA, USA.*
[2]*Technical lead, AI ML researcher, Eudoxia University USA.*
[3]*Cyber recovery Lead, Pacific Gas and Electric, Plano, Texas, USA.*
[4]*Cloud/Data Engineering Expert, DagKnows, Sunnyvale, California, USA.*
[5]*Data and Platform Engineering, American Water, Philadelphia, PA, USA.*
[6]*Software Engineer, Independent Researcher, San Jose, California, USA.*

[1]*Corresponding Author : online.saurav@gmail.com*

Received: 10 February 2024 Revised: 17 March 2024 Accepted: 05 April 2024 Published: 15 April 2024

***Abstract*** *- This study examines the evolving landscape of cybersecurity in the context of Generative Artificial Intelligence (AI), highlighting the dual-edged nature of technological advancements that offer significant potential for innovation while posing new threats to user security and privacy. We critically analyze the mechanisms through which Generative AI facilitates sophisticated impersonation attacks and privacy breaches, underpinned by a comprehensive review of current and emerging threats. By synthesizing recent research, we identify gaps in traditional cybersecurity approaches and underscore the necessity for novel solutions that are adaptive to the complexities introduced by AI technologies. This paper proposes a multidisciplinary framework that integrates technical, legal, and ethical considerations, aiming to fortify digital ecosystems against AI-driven vulnerabilities. Through methodological rigor, we offer insights into authentication and verification mechanisms that promise to enhance user security without compromising privacy. Our contributions extend beyond theoretical analysis, proposing actionable strategies for stakeholders to implement robust defenses against the misuse of AI. By anticipating future developments in AI technology, this study sets the groundwork for ongoing innovation in cybersecurity practices, ensuring they remain effective in the face of rapidly advancing digital threats.*

***Keywords*** *- Generative AI, cybersecurity, Privacy breaches, Impersonation attacks, Authentication, Verification mechanisms, digital ecosystems, Legal and ethical considerations, AI-driven vulnerabilities, Multidisciplinary framework.*

## 1. Introduction

Today, the widespread advancement of technologies such as deep learning has provided ever-growing access to increased computation power. It has become one of the most critical situations for user security and privacy. Specifically, "Generative AI," which is more reliable and accurate, is being developed and implemented these days as it allows synthesizing and creating a large amount of data from a smaller number of inputs. This is a significant advantage compared to traditional AI. However, the capabilities of generative AI in terms of generating authentic content have also led to enormous risks for sophisticated impersonation attacks. In the field of cybersecurity, more and more attacks and threats use AI methods and are becoming smarter and more powerful. With the rise of generative AI, it is very likely that we can expect bigger and more serious AI-oriented attacks in the future, and traditional cybersecurity methods and tools may not be effective in confronting those attacks. Therefore, new research areas focusing on how to improve user security and privacy in the new AI-pervasive age are in demand. Given the risks posed by rogue AI applications, including emerging threats such as those discussed above, it is crucial to understand this activity and consider research that explores safeguarding against such activity in future work. In the next few sections, we will explore many different and multidisciplinary research areas in AI security and develop novel solutions for protecting digital content and user privacy. [1,2,3,4]

### *1.1. Impersonation through Generative AI*

AI systems that can generate photorealistic images are now available to the public. Generative algorithms take in large data sets and "learn" to generate new data with the same statistics as the original set. These have been used to produce realistic images of people, animals, and scenery. Such images are often indistinguishable from real

photographs and videos and will become even more realistic over time. Similar technologies, such as natural language processing algorithms, can be used to create text which imitates the writing style of a specific person. Such technology could enable an attacker to generate an image of a particular individual and then develop writing in a text which appears to be that person speaking - effectively, a form of digital impersonation. There are prominent examples of deepfakes and similar digitally created images and videos being used to produce material designed to mislead or fake public opinion. For example, there have been reports that digitally created footage of political activities has been used to misrepresent events in a particular country. As a result, some countries have passed specific laws that make distributing deep fakes a criminal offense [5]. However, in the UK, the ability of national prosecutors to bring charges in these circumstances has been questioned due to the way in which the relevant statute is drafted. Specifically, the Crown Prosecution Service is required to consider whether it is in the public interest to prosecute and to assess whether a past distribution has caused harm [6]. This can create practical difficulties as, for example, it may be difficult to prove harm at the time when the decision to prosecute is made. Also, given that the technology in question is likely to be constantly developing, there may be significant delays in establishing whether a given file is a "deepfake" or similar, and so the period in which a defendant can be charged may have expired.

### *1.2. Importance of User Security and Privacy*

User security is an important consideration in the development and deployment of generative AI technology, with robust measures necessary to prevent impersonation or misuse of user data. This need is underscored by the increasing volume and variety of personal data being gathered and shared by the users of online services. In recent years, the growth of social media and e-commerce platforms has led to a surge in the availability of user data, providing rich and valuable sources for potential attackers to exploit [7].

Today, ensuring privacy and personal information is secure has been a major focus. However, there is a notable trade-off between the privacy and utility of users' personal information. As new AI technologies emerge, such as deep learning algorithms and adversarial AI, new categories of security threats begin to show, making the task of protecting user identity and privacy increasingly challenging. Despite these emerging threats, regulatory and legislative progress has been limited. It is essential to consider the legal and ethical issues in the use of technology and the extent to which the state and law can protect against the misuse of personal information. With the explanatory work to be done in the field of AI and the increasing public awareness of privacy and data protection, there should be more movements involving both technical and non-technical measures to secure the safety and privacy of the public. The security and privacy measures employed should be justifiable by the nature of the data and the supposed level of risk. All possible aspects of private information and potential misuse of technology should be taken into consideration during the development of AI projects and the implementation of relevant regulations and legislation.

## 2. Challenges with Rogue AI Applications

Generative AI, especially the recent deep learning-based AI models, has shown remarkable advances in generating realistic images, videos, and audio [8, 9]. However, there are significant challenges in terms of user security and privacy. Impersonation through generative AI is a major concern, which refers to the act of an AI or a non-human thing pretending to be a particular human. For instance, an attacker can use a Generative Adversarial Network (GAN) to generate synthetic face images that look like a specific, real person.

In this case, the attacker can create social media accounts or send spam emails by using the synthetic face image to impersonate the victim. Even though there is no public clone with that person's facial image, current deep learning-based AI models can still produce very similar face images that look like that person. Also, with the increasingly deep fake videos generated by AI algorithms, it is now possible to manipulate the facial expressions and the lip movements of a person in a target video, no matter whether the person is a public figure or an ordinary citizen [10]. These videos can be used for various malicious purposes, such as defaming the victim or spreading false information.

Moreover, they are becoming more prevalent nowadays due to the easy access to AI technologies and the widespread use of video-sharing platforms on the internet. Such malicious activities can have harmful consequences for the victim, damage his reputation and cause legal issues. Potential risks to user identity and privacy concerns are discussed elsewhere in this paper. Authentication and verification mechanisms and identity protection measures are suggested.

Both legislators and securities regulators did not anticipate the explosion of AI-driven interactive technology on the internet. High-profile regulator concerns and low-level legislative initiatives have been ongoing since 2018, addressing issues related to deep fakes and AI-driven impersonation [11]. However, as AI technology evolves rapidly, it is challenging to keep pace with the enactment of legislation and regulation around the world, let alone to fully understand the implications of using this technology in-depth. Hence, a pressing research direction is to explore legal and ethical regulatory responses that would strike an appropriate balance between preventing misuse and not unduly intruding upon conventional freedom of communication and expression.

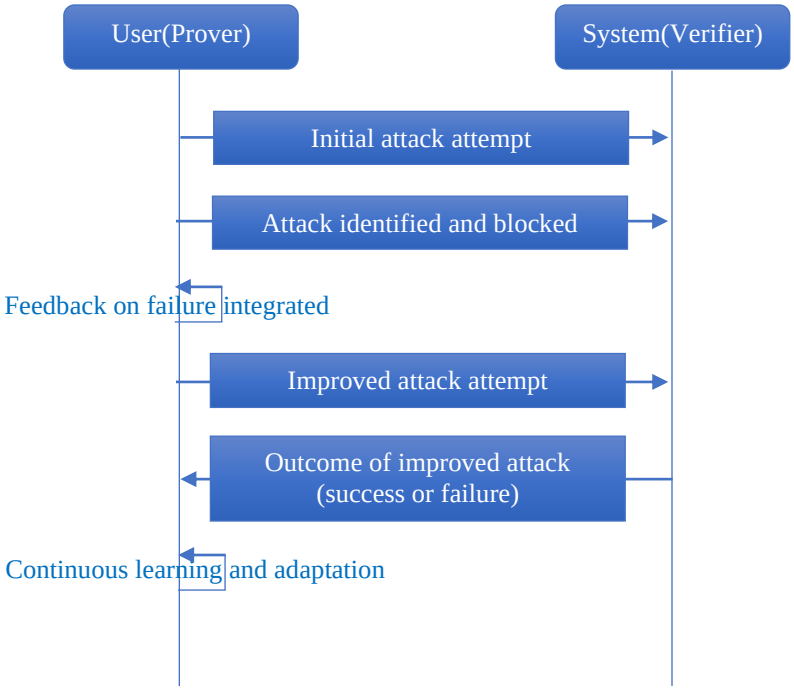


**Fig. 1 Adversarial GenAI improvement on attack iterations**

### *2.1. Emerging Threats*

Looking forward, one key concern for GenAI security is the ability of generative AI to learn about mitigations employed by modern security monitoring tools. In the case of a generative AI being used in an attack, there is a real likelihood that the attack fails, is identified, and blocked, and this outcome is fed back to the generative AI as a learning. Over time, the generative AI generates improved attack iterations that are more likely to bypass the security monitoring tools. An illustration is shown in Figure 1.

It is noted that current machine learning and AI applications have typically been used against traditional signature-based detection systems - that is, systems which search for known string patterns in network traffic and host activities. These detection systems often rely on the presence of an attack having been discovered and analysed before a signature for that attack is distributed to the wider user community. That signature is implemented in security monitoring systems. This means that there is a time window in which attacks can be successfully executed without detection, that is until a signature is distributed and the attack is identified. An illustration is shown in Figure 2.

However, as machine learning and AI are increasingly used to develop advanced evasion techniques, this poses a threat to higher-level anomaly and threat-based detection systems. Such systems, which are employed to identify previously unseen attacks or targeted anomalous behaviours, rely on an ability to compare monitoring output against the system's 'understanding' of what represents normal activity for a given user or network service. The evolutionary potential for generative AI means that it is likely to be more capable of identifying new ways in which it can bypass security features and adapt more effectively whilst under active investigation than traditional, human-led reverse engineering approaches may be able to identify and respond to such threats.

This has consequences for the development of effective security against both known attacks and for the emerging risk of AI bypassing higher-level anomaly detection and preventative monitoring mechanisms. In terms of possible legal and regulatory ramifications, it may be that future liability for inadequate security leading to data breaches might need to reflect a capacity to demonstrate proactive respect for the potential capabilities of AI and generative design in undermining data security measures.

As the UK and EU draw closer to the establishment of the Regulatory Framework for AI, it will become increasingly important for data controllers and processors to take heed of emerging threats from AI and machine learning in practice and be able to demonstrate a capability to assess and respond to risk in an evolving digital threatscape.

### *2.2. Potential Risks to User Identity*

It is important to note that the risks associated with generative AI impersonation represent a significant departure from the traditional digital account takeover. In the case of social media impersonation, victims often face an uphill battle in having fake accounts removed, despite some social media platforms having established reporting functionalities [12]. Such risks to social media users have been documented frequently by researchers, and it is crucial for such risks to be mitigated [13].

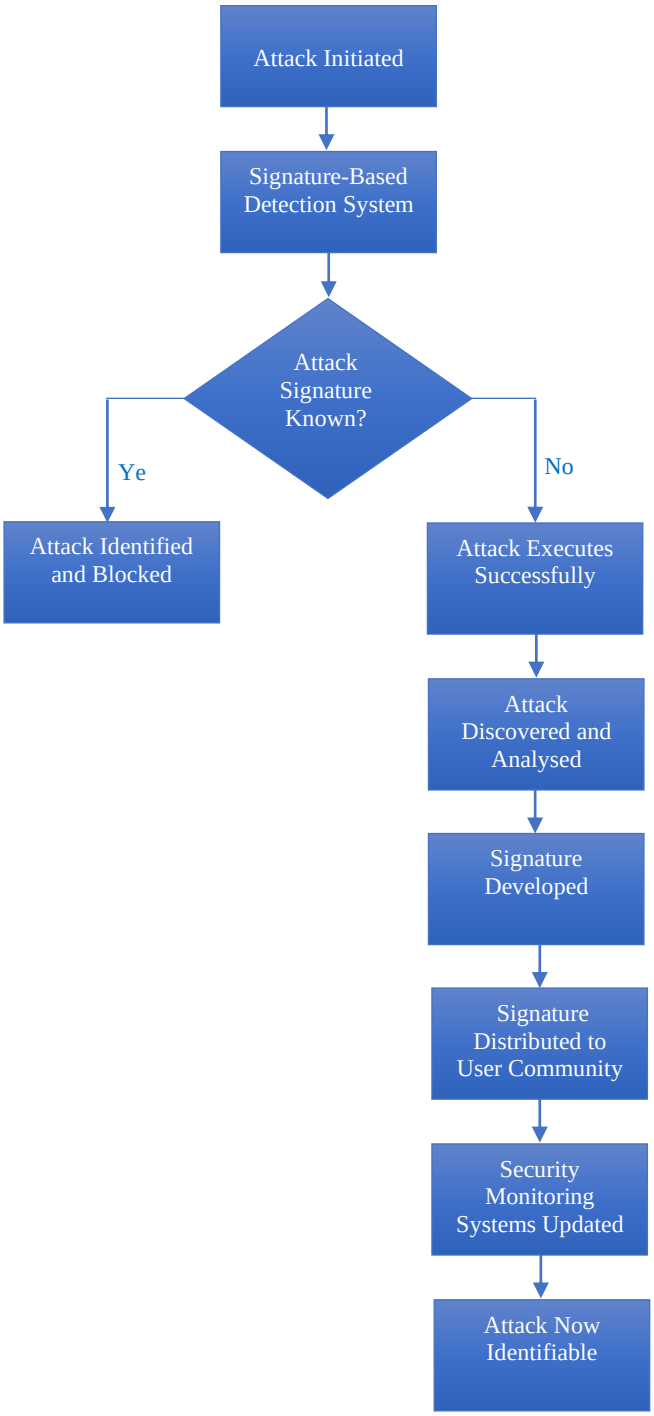


**Fig. 2 GenAI attacks on signature-based detection systems**

In the case of a user's digital identity becoming compromised, issues may arise from the impersonation extending to other services and personal devices. This is an emerging field of research which is receiving growing interest in the academic community. As this attack vector rises, it is becoming increasingly feasible for impersonation not to be used solely for social media disorder; criminals may look to capitalize by using fake identities to engage in financial crime or to abuse and harass a victim's contacts. This kind of 'cross-platform' impersonation represents a severe danger to both the victim and their social circle, as the exposure of a fake identity can have cascading social and professional effects.

Furthermore, the relative anonymity that generative AI applications offer to attackers through impersonation exacerbates the risks to user identity security. For one, it is difficult to trace and prosecute online impersonation committers due to the obfuscatory effects of generative AI. As any possible internet censorship research paper would discuss, the existence of tools and infrastructure which allow for user identity to be hidden makes the task of locating and defending against attack actors considerably harder, if not impossible. Secondly, the very possibility that deep fakes or similar could be used to generate compromising or defamatory content means that victims may be reluctant to seek legal recourse. For example, suppose a victim of digital impersonation has fake indecent visual content shared online. In that case, the ongoing presence of such material during a court case may cause reputational or emotional harm.

### *2.3. Privacy Concerns*

In general, various AI applications have raised privacy concerns among the public. The growing concerns about privacy generally come from the fact that AI effectively makes it easier for governments, companies, and even private individuals to amass, process, and analyse personal data - from social media and other platforms, from data breaches, through face recognition, and in many other ways [14]. The potential for a large, centralized collection of personal data and the possibility of it being misused are at the heart of anxieties. However, it should be noted that the potential privacy concerns appear to be even more severe given the rise of the so-called "generative AI" technology, as compared to traditional AI programs. This is because generative AI has the capability of generating large amounts of fake, yet very realistic, data - creating the possibility that all data, the real ones and the fake ones, would become much less reliable and even more difficult to distinguish from one another.

Consequently, it is expected that new challenges will arise when attempting to protect the privacy of individuals, including the need to develop more advanced strategies to safeguard data privacy. One of the most popular ways to protect privacy is through data anonymization - that is, by either encrypting the data in a certain way that identities are kept secret or scrubbing the data clean of identifiable information. However, it should be noted that many laws, including the European Union's General Data Protection Regulation, set out very strict standards for it to be deemed as a proper anonymization. This means that businesses and individuals may not be able to utilize properly anonymized information in any way they see fit, which may potentially hinder the utility and benefits of big data analysis and AI.

## 3. Ensuring User Security

To ensure user security, the article suggests implementing authentication and verification mechanisms. These refer to all the tools and policies used to ensure that a certain identity, such as a user or a device, is legitimate and not a fraudulent one. For instance, multi-factor authentication can be used, meaning that two or more credentials must be provided to get access. Another widely used method is biometric technology, like fingerprints. This relies on the user being who they say they are and has the bonus of not requiring the user to recall a password. However, these must be securely stored and managed to prevent potential threats. New services are being provided to automatically detect and alert people if their personal information is being exposed or compromised. It is suggested that taking advantage of these services can aid in the fight against identity theft or impersonation using generative AI. However, it is also noted that these solutions use public data as input, and the concept still poses significant threats to individuals' privacy and security. For example, end-to-end encryption for smart devices is a way of preventing rogue AI. This is a method for secure communication that prevents third parties from accessing data while it is being transferred from one end system or device to another. This is different from the at-rest encryption used to secure data on, say, a laptop or a phone.

Further, the specific device users should manage the encryption keys and identity keys to achieve goals in protecting the user's identity. This will impose a huge challenge for rogue AI applications because normally, these AIs must find ways to take over some legitimate users' accounts fully, and encryption can effectively prevent user identity from being misused. Overall, maintaining privacy is an ongoing and never-ending task, one that technical, operational, and business teams need to engage with comprehensively. Social science, humanity, and legislation, etc., also play vital roles in it. For those working in the security technology sector, this is a call to arms - new alliances will potentially arise in the future, with the aim of advocating the user's needs and interests in keeping their personal information private and secure.

### *3.1. Authentication and Verification Mechanisms*

Since it is very difficult to prevent unauthorized manipulations and usage of AI models after they have been released to the public, it is important to verify the identity of the user and the purpose of using the generative AI to prevent misuse of the system beforehand. This problem is being addressed using different methods ranging from traditional password-based authentication techniques to some of the latest biometric and cryptographic technologies. For example, some of the current AI training platforms require the user to show the output of the generative AI with some randomly generated inputs in the web camera to prove that the user is a real person instead of a rogue AI. However, it is questionable whether these methods could make it as most of the public platforms today only employ very basic user authentication procedures due to usability and development complexity concerns [15]. On the other hand, because both the generation of AI and the user authentication process involve complicated algorithms with many factors to be considered, there are no industry standards or common frameworks that could provide live consensus and guidelines on what technologies or methodologies should be employed to ensure the security and the practicality. It is still an open question on how to effectively balance the user's privacy and the necessity of an identity check for any generative AI activities. Finally, in the context of frequent security upgrades and vulnerability patches on popular applications and systems nowadays, the research community and the industrial partners are still struggling to keep the technology up to date for the prevention of misuse of generative AI [14]. It is also anticipated that there will be more intelligent and sophisticated attack methods available to bypass AI user authentication soon, which requires continuous research and studies on the development of new defence mechanisms.

### *3.2. Robust Identity Protection Measures*

Particularly demanding for companies making use of generative AI, comprehensive identity protection measures form a critically important part of any IT security strategy. The impersonation risks that bot-based abuse has brought to the fore over the past few years have demonstrated why such protections should be given heightened significance in an increasingly automated digital world. The focus on keeping real user data private using a combination of tokens and encryption means that the ability of systems to act on behalf of users can easily warrant an entire section in the broader data protection strategy. However, the increasingly theoretical concept of privacy through design [16] - a principle that places emphasis on creating systems with pre-considered, automatic safeguards for personal information - is where machine learning - the technology often underpinning generative AI projects - truly has the potential to provide something groundbreaking. For researchers and developers looking to improve existing automated identity protection measures, developments in AI technology are both an exciting opportunity and a tantalizing challenge - and thanks to the broad, potentially game-changing nature of the work, funding for projects in this field is increasingly common. The capacity of generative AI to replicate human output convincingly is continually improving each year. However, it is crucial for the development of protective measures and approaches to stay abreast to preserve user trust and confidence in the security and reliability of online platforms.

### *3.3. Safeguarding User Privacy*

Safeguarding and ensuring user privacy is an essential issue in every piece of AI application. In the case of generative AI, the risk is even higher as there is a genuine possibility that user privacy is at stake. To protect safeguards

applicable for user privacy, one possible solution is by rigorous impact assessment with ethics inclusions. This will allow humans and AI to live together peacefully, ensuring that there will be no interference with AI's activities in human life. Also, it is significant to ensure that AI development and deployment across different types of data or applications, particularly generative AI, is subject to its own tests with relevant regulations. This is another way to ensure AI has no negative effects on humans and minimizes their interference in every aspect of societal living. The new AI and Robot rules and standards in the European Union [17], including proposed frameworks for ethical and legal implications for AI development in the UK, are to be seen as a good start in protecting fundamental human rights. Finally, the establishment of a corresponding new industry for AI inspection technologies and services is important to maximize user privacy. As AI or generative AI may have updates from time to time, inspections of AI should be regular to ensure it is kept at the level of protection for both user privacy and security. Also, impact assessments will be legally required, and therefore, new types of jobs requiring knowledge of ethics and law in AI development will be created accordingly. This will boost the benefits to society as it creates business and job values for the development of AI ecosystems. Through the implementation of such effective safeguards, as proposed above, could help increase public confidence and trust in AI and, in return, speed up the adoption process at the market level.

## 4. Conclusion

### *4.1. Anticipating New Forms of Rogue AI*

The complexity involved in developing a rogue AI, combined with the relatively high risk and potentially severe consequences, such as privacy breaches and loss of public trust, suggest that truly effective new security technologies would be valuable. However, identifying fruitful directions for research and development in this area may be challenging. A more interdisciplinary approach is necessary not only involving AI and computer science experts but also legal and ethics scholars and the public and private enterprises and governmental departments that will have an interest in maintaining public trust in the identity and authenticity of digital media and communication. Securing against rogue AI is not the responsibility of a single group or research area but will involve a coordinated effort across various disciplines. Interconnected, multidisciplinary approaches – a phenomenon referred to as cyber security by design where the whole technical environment, including all software, hardware, and social interfaces, together with methods and procedures, are considered essential to anticipate and mitigate new forms of rogue AI.

This is a holistic and future looking view, building in privacy, security and information assurance as an interdisciplinary requirement that should start at the beginning of any system or technology lifecycle from design right the way through to decommissioning. So, the idea of cyber security by design is a further affording point in the context of protecting against future AI threats, with this being a necessary development that should see far greater attention and funding considering the potential impacts that could occur from future rogue AI problems. This is particularly the case given that current approaches to user privacy and security – such as data protection – are very legalistically formalistic, where various compliance steps and technical measures may satisfy the formal requirements of legal rules without protecting a system from attack.

### *4.2. Advancements in Security Technologies*

Besides the various biometric-based approaches, there has been an increasing research interest in AI-driven security solutions. Considering the numerous emerging threats and vulnerabilities, the utilization of AI technologies to develop automated and adaptive security systems could potentially bring forth significant improvements in cybersecurity. For example, AI could be employed to help in the automatic identification of new cybersecurity threats and risks, thereby allowing the system to adapt its defence mechanisms in response to these risks autonomously. Another potential of AI applications is the utilization of big data analytics in enhancing cyber threat intelligence, which is vital in understanding the constantly evolving threat landscape in cyberspace. By analyzing the massive volume of data generated from multiple sources in real-time, AI-driven big data analytics could help to predict and prevent future cyber-attacks more effectively [18].

### *4.3. Collaborative Efforts for Enhanced User Protection*

In recognition of the potential impact of the security risks posed by impersonation through generative AI on society, industry, and politics, we have seen a proliferation of private and public sector organizations that wish to contribute to tackling these challenges. Given the scale and complexity of the issue, it is common ground that effective action will require collaborative and coordinated efforts, which will need to span from the development of new technical and legal standards to the reshaping of public understanding of digital and AI-mediated activities and identities. It is also noteworthy that interdisciplinary work between different fields, such as computer science, law, and digital sociology, is essential to appreciate the nature of these risks fully and to formulate effective responses.

National regulators, multilateral institutions and other international bodies will all have an important role to play in ensuring that there is a consistent and rigorous level of supervision, including the enforcement of penalties for those who fail to meet the required standards. This will be crucial not only for managing the risks posed by existing uses of generative AI but also in laying the groundwork for the introduction of more sophisticated security measures and the continued expansion of AI technologies into different areas

of industry and society. Lastly, given the potential for these issues to be driven by commercial dynamics in a global marketplace for AI-related goods and services, efforts to engage in thoughtfully and reciprocally shaping regulatory environments across different territories is an important consideration for the future. It will be necessary for both national and international actors in generative AI security to navigate and grapple with the challenges of harmonizing diverse and evolving policy and regulatory landscapes.

By working together to create the conditions for a secure, safe, and trusted digital ecosystem, we can ensure that generative AI technologies can be harnessed to create powerful new tools for human expression, creativity, and discovery - whilst safeguarding individual identity and privacy.

## Funding Statement

This publication was funded by a grant from The New World Foundation.

## Acknowledgments

We want to extend our heartfelt thanks to Pradeep Chintale, Cloud Solutions Architect, SEI Investment Company, Downingtown, Pennsylvania, United States and Ravi Soni, Smart Manufacturing & Transformation Leader, Houston, Texas, US, for their insightful comments and constructive feedback on our manuscript. Their expertise and thoughtful critique have significantly contributed to the enhancement of this work. We deeply appreciate the time and effort dedicated to reviewing our paper and guiding us toward a more rigorous and polished final product. Thank you.

## References

[1] Emilio Ferrara, "GenAI against Humanity: Nefarious Applications of Generative Artificial Intelligence and Large Language Models," *Journal of Computational Social Science*, pp. 1-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Nektaria Kaloudi, and Jingyue Li, "The AI-Based Cyber Threat Landscape: A Survey," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1-34, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Brandon Khoo, Raphaël C.W. Phan, and Chern-Hong Lim, "Deepfake Attribution: On the Source Identification of Artificially Generated Images," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 12, no. 3, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Taís Fernanda Blauth, Oskar Josef Gstrein, and Andrej Zwitter, "Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI," *IEEE Access*, vol. 10, pp. 77110-77122, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Edvinas Meskys et al., "Regulating Deep Fakes: Legal and Ethical Considerations," *Journal of Intellectual Property Law & Practice*, vol. 15, no. 1, pp. 24-31, 2020. [Google Scholar] [Publisher Link]

[6] Benjamin Widdicombe, "*Decision-Making in the Crown Prosecution Service: How do Prosecutors Make Case Decisions?*," Apollo - University of Cambridge Repository, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Ankit Kumar Jain, and B.B. Gupta, "A Survey of Phishing Attack Techniques, Defence Mechanisms and Open Research Challenges," *Enterprise Information Systems*, vol. 16, no. 4, pp. 527-565, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Yihan Cao et al., "A Comprehensive Survey of AI-Generated Content (AIGC): A History of Generative AI from Gan to ChatGPT," *arXiv preprint arXiv:2303.04226*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Nantheera Anantrasirichai, and David Bull, "Artificial Intelligence in the Creative Industries: A Review," *Artificial Intelligence Review*, vol. 55, pp. 589-656, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Hany Farid, "Creating, Using, Misusing, and Detecting Deep Fakes," *Journal of Online Trust and Safety*, vol. 1, no. 4, pp. 1-33, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Shalini Rai, "*Legal Liability Issues and Regulation of Artificial Intelligence*," Dissertation, 2023. [Google Scholar] [Publisher Link]

[12] Ankit Kumar Jain, Somya Ranjan Sahoo, and Jyoti Kaubiyal, "Online Social Networks Security and Privacy: Comprehensive Review and Analysis," *Complex & Intelligent Systems*, vol. 7, pp. 2157-2177, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] John A. Naslund et al., "Social Media and Mental Health: Benefits, Risks, and Opportunities for Research and Practice," *Journal of Technology in Behavioral Science*, vol. 5, pp. 245-257, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Yuantian Miao et al., "Machine Learning–Based Cyber-Attacks Targeting on Controlled Information: A Survey," *ACM Computing Surveys*, vol. 54, no. 7, pp. 1-36, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Alessio Rugo, Claudio A. Ardagna, and Nabil El Ioini, "A Security Review in the Uavnet Era: Threats, Countermeasures, and Gap Analysis," *ACM Computing Surveys*, vol. 55, no. 1, pp. 1-35, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] A. Michael Froomkin, and Zak Colangelo, "Privacy as Safety," *Washington Law Review*, 2020. [Publisher Link]

[17] Daniel J. Solove, and Paul M. Schwartz, *Consumer Privacy and Data Protection*, 2023. [Google Scholar] [Publisher Link]

[18] Senthil Kumar Jagatheesaperumal et al., "The Duo of Artificial Intelligence and Big Data for Industry 4.0: Applications, Techniques, Challenges, and Future Research Directions," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 12861-12885, 2021. [CrossRef] [Google Scholar] [Publisher Link]