



TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Digital Privacy in the Age of AI: Protecting Your Identity in a Smart World

In the modern world, intelligence is no longer limited to humans; machines are now able to watch, learn, and anticipate every digital action we take. This poses an important question: are we really in charge of our privacy, or are we only witnessing its gradual erosion?

Saman Khalid | Computer Science Student | Published: June, 2026

✉ Saman819khalid@gmail.com | Position: Student

Introduction

In the era of artificial intelligence — every click, search, and online interaction creates a digital footprint that is more valuable than ever.

The emergence of large language models (LLMs) and the chatbots that go along with them, together with the AI boom, presents new privacy problems. Does a model's training data contain our personal information? Does law enforcement have access to our prompts? Will chatbots link disparate threads from our virtual life and produce them for anybody? **[1]**

Artificial intelligence (AI) has become a part of our everyday life in ways we may not even be aware of in recent years. It has spread so widely that many people are still ignorant of its effects and how much we depend on it.

Face ID and picture recognition, emails, applications, social media, Google search, and digital voice assistants are just a few of the AI services we can access as soon as we turn on our devices. Thus, the majority of our everyday lives are directly impacted by AI **[2]**.

However, privacy concerns are more urgent than ever due to the exponential growth in the amount of data we create and exchange online. I believe it is crucial to investigate the subject of privacy in the age of artificial intelligence and examine how AI affects our private information **[3]**.

“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.” — Edward Snowden

Technology Overview

It's critical to first comprehend how AI functions in our daily lives in order to comprehend why privacy is at risk. The practice of safeguarding private or sensitive data that AI gathers, uses, shares, or stores is known as AI privacy **[4]**.

AI is the capacity of a machine to exhibit human-like characteristics including learning, thinking, planning, and creativity **[5]**. Without being specifically trained for every situation, AI systems learn



from enormous volumes of data by spotting patterns that allow them to make predictions or conclusions. Consider it like teaching a computer by providing it with a million instances rather than a million rules [6].

A lot of us already use AI systems, sometimes without even realizing it. For instance, AI frequently works in the background to produce results and provide a brief description of the material we're seeking for when we use an online search engine [7].

All of the data that users enter into a chat box is gathered by generative AI assistants like ChatGPT and Google Gemini. To enhance the AI model, each query, answer, and prompt that users input is captured, saved, and examined. Sometimes people are unaware that their data is being collected [8].

As technology has advanced, digital privacy has also changed. Privacy issues were confined to social networking sites and email in the early 2000s. Large volumes of personal data are being gathered via wearable technology, smart home systems, smartphones, and AI-powered apps [9]. The main purpose of data input into AI systems is to train models and improve their functioning, however this raises serious privacy issues for users [10].



Figure 1: A surveillance camera watching a public crowd, representing public worry over AI and data privacy.

Key Findings & Impact

Broadly, Malwarebytes found that: 89% of people are “concerned about my data being used by AI tools without my consent.”[11].

Artificial intelligence has subtly become a part of our everyday lives. These are only a few instances of how AI is being used in daily life to influence how we live, work, and communicate [12]. As soon as we turn on our gadgets, we immediately access AI features like:

- Image recognition and face identification



- Emails, applications, and social media
- A Google search digital voice assistants such as Alexa from Amazon and Siri from Apple
- Internet banking
- Driving aids include weather information, traffic updates, and route mapping.
- Purchasing
- Leisure time, like Netflix and Amazon for films and TV shows. [2]

The current state of privacy protection may need to be reviewed due to the growing usage of AI, but this does not imply that privacy will disappear or become obsolete. The development of socially conscious AI will be aided by striking a balance between technological innovation and privacy concerns. [13]

What's Next?

The legal, ethical, and technological issues around AI and data privacy are extremely complex [14]. AI systems handle previously unheard-of amounts of personal data, posing privacy issues that go much beyond those of conventional software. Organizations have difficulties in safeguarding sensitive data while utilizing the potential advantages of these formidable technologies as artificial intelligence develops and becomes more essential to commercial operations [15].

1. How to Maintain Your Privacy in an AI World?

Recognize What You Share: AI-driven apps frequently ask for personal information. Examine permissions thoroughly.

2. **Utilize Privacy Settings:** Make use of the options that many platforms provide to restrict data collecting.

3. **Enable Robust Security:** To safeguard accounts, use Multi-Factor Authentication (MFA) in conjunction with strong passwords.

4. **Keep yourself informed:** by learning how your data is handled by AI systems. Transparency is essential.

5. **Think Before You Click:** Steer clear of excessive social media sharing and use caution when using AI tools or chatbots.[16]

There is no denying the illusion of privacy in the AI era. But that doesn't mean we have to give up. While complete privacy might be unattainable, improved privacy is possible. We can have more control over our data by being aware, making wise decisions, utilizing the right tools, and applying pressure for systemic reforms [17].

About the Author

Saman Khalid is a Computer Science student focused on AI and future systems. She can be reached at Saman819khalid@gmail.com

Keywords: Artificial Intelligence; Cybersecurity; Data Privacy; AI Powered threat; Pakistan Tech



References

- [1] Billiris, G., Gill, A. and Bandara, M., 2025. Privacy in the Age of AI: A Taxonomy of Data Risks. *arXiv preprint arXiv:2510.02357*.
- [2] University of York (2025) Artificial intelligence and its impact on everyday life. *Online York*. Available at: <https://online.york.ac.uk/resources/artificial-intelligence-and-its-impact-on-everyday-life/>.
- [3] van Rijmenam, M. (2023) Privacy in the Age of AI: Risks, Challenges and Solutions. *The Digital Speaker*. Available at: <https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/>.
- [4] IBM (2024) Exploring privacy issues in the age of AI. *IBM Think*. Available at: <https://www.ibm.com/think/insights/ai-privacy>.
- [5] European Parliament (2020) *what is artificial intelligence and how is it used?* Available at: <https://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used>.
- [6] European Google Cloud (no date) *what is Artificial Intelligence (AI)?* Available at: <https://cloud.google.com/learn/what-is-artificial-intelligence>.
- [7] CELCIS (2025) *what is AI? Understanding Artificial Intelligence in your daily life: a brief introduction to AI*. Available at: https://www.celcis.org/application/files/9017/6475/8247/A_brief_introduction_to_AI_transcription.pdf.
- [8] The Conversation, 2025. AI tools collect and store data about you from all your devices – here's how to be aware of what you're revealing. Available at: <https://theconversation.com/ai-tools-collect-and-store-data-about-you-from-all-your-devices-heres-how-to-be-aware-of-what-youre-revealing-251693>.
- [9] FundsforNGOs (n.d.) *Sample proposal on digital privacy concerns in the modern age*. Available at: [Sample Proposal on Digital Privacy Concerns in the Modern Age](#).
- [10] Syrenis (2024) *Data privacy in the age of AI: Challenges and solutions*. Available at: <https://syrenis.com/resources/blog/data-privacy-in-the-age-of-ai/>.
- [11] Ruiz, D. (2025) '72% of people are worried their data is being misused by the government, and that's not all', *Malwarebytes News*, 9 April. Available at: <https://www.malwarebytes.com/blog/news/2025/04/72-of-people-are-worried-their-data-is-being-misused-by-the-government-and-thats-not-all>.
- [12] Edington, M. (2025) 'Examples of AI in Everyday Life: The Unforeseen Impact on Society', *Balto AI Blog*, 12 February. Available at: <https://www.balto.ai/blog/how-ai-already-impacts-our-lives-in-unforeseen-ways/>.
- [13] Office of the Victorian Information Commissioner (OVIC). (n.d.). *Artificial Intelligence and Privacy – Issues and Challenges*. [Online]. Available at: <https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/>.
- [14] The Legal School (n.d.) *AI and Data Privacy: Challenges, Opportunities & Legal Insights*. Available at: <https://thelegalschool.in/blog/ai-and-data-privacy>.
- [15] Delev, Z. (2025) AI Privacy Risks and Data Protection Challenges. *GDPR Local*, 3 July. Available at: <https://gdprlocal.com/ai-privacy-risks/>.
- [16] University of Delaware (2026) *Privacy in the Age of AI: Why it matters more than ever*. Secure UD Threat Alerts, 28 January. Available at: <https://sites.udel.edu/threat/2026/01/28/privacy-in-the-age-of-ai/>.
- [17] DeepFa (2025) The illusion of privacy in the age of AI: nothing remains hidden. *DeepFa Blog*, 4 October. Available at: <https://deepfa.ir/en/blog/illusion-of-privacy-in-ai-era>.