

Works cited

1. OWASP Top 10 for LLM Applications 2025 – OWASP, accessed Mar 10, 2025, <https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/>
2. Bias of AI-generated content: an examination of news produced by large language model – Nature Briefing, accessed Mar 10, 2025, <https://www.nature.com/articles/s41598-024-55686-2>
3. Hallucinating Law: Legal Mistakes with Large Language Models are Pervasive – Stanford University, accessed Mar 10, 2025, <https://hai.stanford.edu/news/hallucinating-law-legal-mistakes-large-language-models-are-pervasive>
4. Researchers Highlight How Poisoned LLMs Can Suggest Vulnerable Code – DARKREADING, accessed Mar 10, 2025, <https://www.darkreading.com/application-security/researchers-turn-code-completion-llms-into-attack-tools>
5. It's true, LLMs are better than people – at creating convincing misinformation – The Register, accessed Mar 10, 2025, https://www.theregister.com/2024/01/30/llms_misinformation_human/
6. Ensuring Student Safety and Data Privacy in Online Tutoring: Essential Guidelines and Best Practices – Caddell Prep, accessed Mar 10, 2025, <https://caddellprep.com/live-online-tutoring/student-safety-and-data-privacy/>
7. Measures & Data Collection – National Student Support Accelerator, accessed Mar 10, 2025,

<https://studentsupportaccelerator.org/tutoring/data-use/measures-data-collection/student-data-privacy-guidance>

8. AI Chatbots Can Guess Your Personal Information From What You Type - Wired, accessed Mar 10, 2025,

<https://www.wired.com/story/ai-chatbots-can-guess-your-personal-information/>

9. Caution: use of AI chatbot may lead to data breaches - Dutch DPA, accessed Mar 10, 2025,

<https://www.autoriteitpersoonsgegevens.nl/en/current/caution-use-of-ai-chatbot-may-lead-to-data-breaches>

10. [Exclusive] Concerns Become Reality... Samsung Electronics Unlocks ChatGPT, Abuses Plunge - The Economist, accessed Mar 10, 2025,

<https://economist.co.kr/article/view/ecn202303300057>

11. LLM03:2025 Supply Chain - OWASP, accessed Mar 10, 2025,

<https://genai.owasp.org/llmrisk/llm032025-supply-chain/>

12. A news site used AI to write articles. It was a journalistic disaster - The Washington Post, accessed Mar 10, 2025,

<https://www.washingtonpost.com/media/2023/01/17/cnet-ai-articles-journalism-corrections/>

