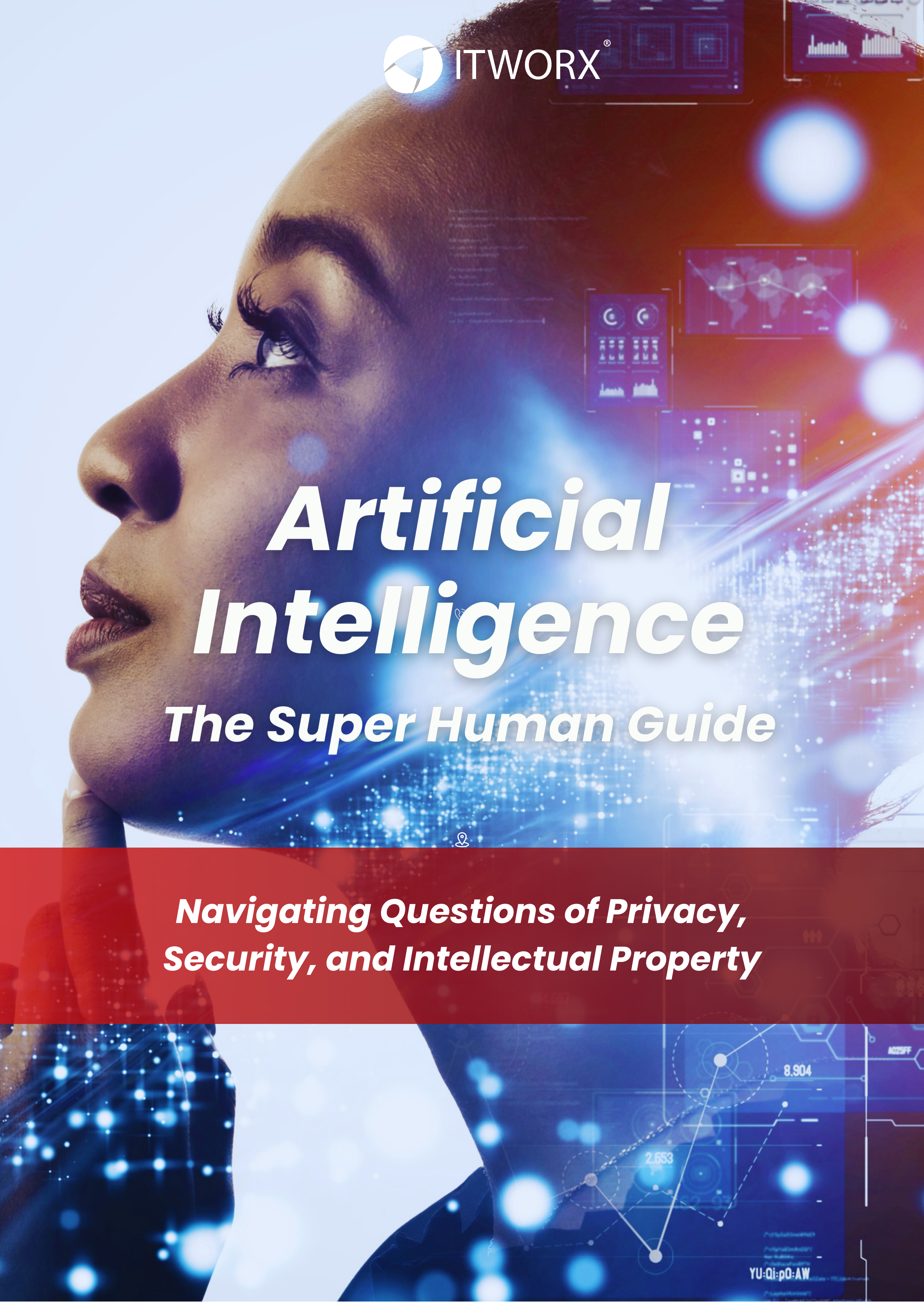
ITWORX®



# Artificial Intelligence

## The Super Human Guide

### *Navigating Questions of Privacy, Security, and Intellectual Property*

## ***Navigating Questions of Intellectual Property & Misrepresentation***

When creating content – for a research paper, market research, a social media caption, etc. – content creators need to cite the sources they have used, if any, to ensure they are not infringing upon existing laws that govern intellectual property. For example, let's say you are writing a report and have correctly cited the Wall Street Journal as a source of information. You are not infringing upon any laws related to intellectual property. If you, however, were to copy/paste the textual content of the WSJ article into ChatGPT and prompt the Chatbot to "paraphrase the text" or to "alter its tone-of-voice to a less formal tone," we get into the turbulent legal territory.

**Who is now the owner of this text/content?**

Is it my original content (because technically, I asked ChatGPT to alter its tone of voice and produce new content ultimately)?

Is it unoriginal content (because technically, I have paraphrased an existing resource, and this typically warrants citations to avoid legal claims of plagiarism/ intellectual property violations)?

***When the EU's European Commission asked about ChatGPT issues related to authorship and content ownership, here is what the chatbot had to say...***

*"I do not own the content that I generate. I am a machine learning model developed and owned by OpenAI, and the content generated by me is subject to OpenAI's license and terms of use."*

## ***Navigating Questions of Intellectual Property & Misrepresentation***

ChatGPT states that the generated content may be copyrighted but does not belong to the AI itself.

In other words, the answer/generated output may be subject to copyright protection, depending on whether it can be considered a "work" that expresses the original views of an author or reflects uniquely creative content owned by the author in question.

Artists and creators who currently use AI to support their creative process may be able to claim ownership of their work if it reflects their choices and creativity. On the other hand, for common commands like “write me a song", ChatGPT will generate content. without the user actually making any creative choices. In the former case, a copyright claim may be viable; in the latter case, it is highly doubtful.

Additionally, there are legal concerns about the misrepresentation of information:

Suppose I use ChatGPT to generate a perfect Cover Letter. Is this a fair, ethical, and legal way to transparently showcase my abilities to a hiring manager? Am I "working smart," or am I misrepresenting the truth about myself and the capabilities needed for the job? To what extent is an AI-generated/perfected CV and Cover Letter a true reflection of who I am as a person to the hiring manager? If, for example, I am not a friendly person, yet I have prompted ChatGPT to "alter the tone-of-voice in my Cover Letter," then where do we legally draw the line between editorial help/guidance and misrepresentation of information?

## ***Navigating Questions of Data Privacy & Information Security***

In addition to concerns related to legality, in the era of generative AI, we need to ensure that our data is adequately secured. Unless you use an AI tool or software, you are 100% sure you won't be using/sharing your data with others. It would be best to assume that your data is not private but will be publicly available to others, used in AI data sets, or even unencrypted for others to read.

Having said that, and with the significant number of AI tools that are available already (more than 1600 different AI tools by the time of writing this article and still counting), then there are specific precautions that you need to take to prevent your data privacy, your employer data confidentiality, and your client's data confidentiality.

These precautions ensure that you use the Artificial Intelligence (AI) tools in a secure, responsible, and confidential manner consistent with the security best practices.

While all these questions may not currently have a single and clear answer – as legal frameworks typically move slower than technological updates/leaps – understanding/dealing with these concerns requires the existence of a content creator/prompt engineer who is familiar with the best practices needed to ensure intellectual property laws are not breached while ensuring that sensitive data is adequately secured. As such, you are responsible for exercising caution and good judgment when working with AI tools, and - as usual - we are here to help you and guide you!

## Overcoming Errors
## &
## Bias

AI tools are prone to errors and bias and should be used cautiously. They are not meant to replace humans; human input is always needed. As such, AI suggestions must be carefully reviewed and verified before use.

## Data Privacy
## &
## Security

Personal data and private/confidential information may not be shared with AI language models, as they may lack safeguards or mechanisms to ensure confidentiality and security.

***AS SUCH, YOU MAY NOT:***

1. Share with AI tools any personal data, including but not limited to names, phones, email addresses, ID numbers ... etc.
2. Share with AI tools you work for, have a business relationship with your employer or have your input related to your employer.
3. Share with AI tools the business relationship with your employer, your clients, and any other information about your employer clients.
4. Share with AI tools any sensitive data or information, whether data that belongs to your employer or its clients. This includes project names and the used technology stacks.

When collecting and processing user data for AI applications, users should ensure compliance with applicable privacy laws and regulations. Personal data should be handled securely and used only for the intended purposes with user consent, where required.

## Notes for Developers

If you are a developer, you may freely share any open-source code with AI tools, but take care while sharing any source code owned by your employer or clients.

In case the developer agrees with their manager to share source code with AI tools for code review or enhancement, they will have to ensure that all usernames, passwords, DB connections, server connections, URLs, URIs, server paths, and other sensitive or confidential data are replaced with simulated data. This step is essential to protect the code's confidentiality and security. Developers may only execute or use AI-generated code on the employer or clients' systems or use any content generated from AI tools if it has been thoroughly inspected and vetted through appropriate processes, procedures, and security tests and measures.

## What to do if you get suspicious?

If you suspect or experience any cyber threats or information leakage due to using AI tools, you must immediately report the incident to your company's infrastructure or security teams. Prompt reporting can help prevent further damage and ensure appropriate measures are taken to address the issue.

In some instances, your employer and through the proper channels, may agree with its clients on the broader use of AI tools; such use may be acceptable only within the agreed-upon terms and limits. Before implementation, the appropriate management and legal team must carefully document and approve any exceptions.

ITWORX®

**We make the world a better place for everyone!**

https://www.itworx.com/

**Contact Us!**