Cutting through the Hyper Sensitivity of OpenAI's ChatGPT-4 AI Generation

By Mark O’Connor, CPA, CMA

Mark has over 30 + years of experience in Financial Management, technology business development and change management. He has advised governments and business clients in building their business technology architecture, their processes, and their data. He qualified as a CPA, CMA with the office of the Auditor General of Canada.

Several technology veterans, for example Microsoft founder Bill Gates, have suggested that ChatGPT is the next big defining moment in technology. Could this be as big as the Internet itself? Could this be as big as the ubiquitous use of spreadsheets for financial analysis, forecasting and analytics? Could this make written documentation available world-wide in up to 95 languages?

The hype of this new tool has several business leaders who also signalling dangers of moving too fast and even risking or dooming the human race. These billionaire leaders include those with direct or indirect investment into the research to the development of the releases of OpenAI’s Chat GPT. Both types of these leaders are proponents of their polar stances and may have business interests and influences in each of their public stands and product announcements.

The hype has become dramatic, and the rhetoric sounds suspiciously like an influencer’s conspiracy theory as it evolves in the media and in the history of the technology and the control of this product. If we attempt to cut through the hype, we see that these leaders all agree that those chat-bots functions will be it is or will be a great way to:

1. Make brief, concise, and clear summaries of large documents in several languages.
2. Save in the creation of technical documentation.
3. A way to quickly assemble disparate documents, policies, processes.
4. Automate and consistently provide customer assistance with company products and services, while adapting dynamically to feedback.
5. Use in education and business management forums either now or when it has been proven to be safe, unbiased, up-to-date history wise and ethically trained and produced. Or to train, control, normalize or socialize to a way of thinking or form a preferred ideology?

OpenAI's ChatGPT-4, a chatbot system uses AI based machine learning approach build collections of text documents to train a bot to generate text into a conversation or banter. AI training uses a Large Language Model (LLM) which holds and indexes a very large quantity of appropriately phrased sample of unstructured text data (e.g., a narrative technology or process description or story). This AI LLM expertise data is used to generate responses to queries made to the Chat-bot.

The intention is that the documents produced are deemed, by proponents, to be public domain and should not in, under these assumptions, be in violation of copyright. Therefore, this is not plagiarized.

Microsoft Release Announcement February 28th 2023; Bing and ChatGPT and Windows 11

SOON HUNDREDS OF MILLIONS OF WINDOWS 11 USERS CAN GET ACCESS TO THIS INCREDIBLE NEW TECHNOLOGY TO SEARCH, CHAT, ANSWER QUESTIONS AND GENERATE CONTENT FROM RIGHT ON THEIR WINDOWS TASKBAR.

Some educators, weighing into their plagiarizing concerns, are using ChatGPT detectors to catch students, or reduce marks for using CHATGPT when it has been banned as a tool by the institution or teacher. The same argument was made, in the day, for calculator use during an examination.

The ultimate responsibility, as per proclamation from OpenAI Chat GPT-4, is that protecting copyright rests with the individual producing the text narrative and their organization publishing the AI generated document. Since the GPT versions are so new, it is unlikely Generated AI copywrites have been effectively tested in the courts. Our initial and early testing findings on just a few cases found that generated text and diagrams have minimal references of source documents available to verify the proclaimed responsibility for copywrite protection. Many of our internet-based research tools normally use references to allow for confirmation and exploration of ideas. A good example is Wikipedia.

Chat GPT is in a test mode therefore caution is important in some cases. We have several questions. This may be one of the largest public technology tests conducted. Until better and fully transparent testing is done, published and accepted, could user's trade secrets, private or classified data be supplied to populate the LLM? Could a browser or applications supplementing LLMs latch on to ChatGPT queries? Could there be LLM additions made which contain market information or private information that is not intended for disclosure? It could be important, during this early testing, to try to get assurances for protecting your data or avoid using ChatGPT intake processes with sensitive, private or confidential information. It is a good practice in testing this tool to review ChatGPT query response for inappropriate disclosure before distribution or publication of your generated text.

Documents used in the base LLV document set are generally sourced from the Web. The LLM patterns and content are used to communicate the ideas, as well as process facts and knowledge. ChatGPT-4 contains data that can be dated or out-of-date by a couple of years. Therefore, it is already dated and incomplete content. We are told in the details we have that GPT-4 does not contain current history about visionaries, obituaries from the daily news, or tweets. We don't know what GPT generally knows and what it does not know.

In our research and case testing of ChatGPT-4, we made some queries of the local building code requirement for a beam span material and sizes. The query responded with a reference to a table in the Building Code of Ontario (which was noted but not provided). No further simple ChatGPT queries for the table would produce the values in that published table. That key table is probably not posted in the internet as it is somewhat guarded from being used by qualified professionals. The Building Code book must be purchased or borrowed from the public library, in this case, because the regulations intend that a qualified person, probably with building engineering credentials or training, read and to safely interpret the data – the old saying being that a little knowledge can be a dangerous thing.

Without strict control, standardization and assurance from the Chat-bot suppliers there are risks and concerns of the chance that bots causing damage.

Based on how new this is, few people have a grasp of what GPT can or cannot do. What is not transparent and not independently assured at this stage of the AI applications are details about:

- The actual content of the training models. The content inclusions and exclusions, any biases and any private information that could be present or extracted from user AI training material content and later used by the public LLM. We do have vague claims from the developers but not yet independent assertions. This April 2023 The Canadian Federal Privacy Watchdog announced that they are probing OpenAI ChatGPT technology for the possibility of potential personal privacy breaches of this type. The US Federal Trade Commission is also investigating of similar complaints.
- How do we know that the LLM material is politically, religious and culturally neutral and not aligned with any particular extremities? Can certain lobby groups, parties, industries, companies, hedge funds and public relations groups intentionally add their own “spin” through supplementing with their own LLM training?
- Testing performed and certification assurance provided help to ensure that confidential trade secrets or private information are not disclosed in the LLM.
- Are there assurances that there are no inappropriate and deceptive biases introduced into the Chat-bot responses?
- In the case of dynamically updated LLM training, as in browser-addon versions of the Open AI base the users own, email could be used in the chatbot training.
- It has been difficult for some public AI Chat services to keep up or scale up to ChatGPT-query demand. Google has added their own ChatGPT as an addon to the Chrome Browser while Microsoft has their AI chat in Bing. The Twitter-Tesla group has indicated that it is independently working on its own AI Chat bot.

At this stage, given these concerns, the tool should be used with these aspects, factoring in and with consideration for, disclosure business risks.

While there is general agreement that the ChatGPT AI Generation method is extremely powerful, easy to use and a game changer, some industry ethical and safety advocates, government agencies and individuals who that the there has not been enough testing. There are calls for a moratorium of new versions of ChatGPT for the next six months or until weakness are identified published and, where possible, resolved.

Like with any new technology, there will be early adopters/evangelists, those who will never use the technology and those who need conclusive demonstration of a return on investment and the technology's safety.

Architect the Company's Machine Learning

Large or forward planning organizations may want to architect there own AI ChatGPT LLV version that automatically injects their organization's ideology and business caring culture into the process guides and communication generation.

Adopting a new way to work and Change Management

Like any new technology there will be early adopters / evangelists, those that will never use the technology, and those that need conclusive demonstration of a return on investment and technology's safety. If you try to use the product for a small non-critical safe use case and document the objectives and effects you can quickly establish a well informed position on this fundamental change to your business and skill experience.

Try it for Yourself

The following links can help you to phrase your queries to achieve the kind results that you aspire to. At the time of publication, free for trial:

- CHATGPT from OpenAI -https://chat.openai.com/chat.
- Addon to your Chrome browser: https://merlin.foyer.work/.