



Informational Bulletin 24-01

Artificial Intelligence (AI): MCPD Best Practices

Date: March 25, 2024

This Informational Bulletin aims to inform Montgomery County Department of Police (MCPD) employees/team members of the emerging capabilities of Artificial Intelligence (AI) and caution members against some of its inherent dangers. The Bulletin aligns with recent MCG recommendations developed by the Technology and Enterprise Business Solutions (TEBS).

To prioritize safety, protect our agency, and safeguard law enforcement data and information while utilizing Artificial Intelligence (AI) tools, best practices guide that individuals should keep these guidelines in mind while using Artificial Intelligence (AI) Large Learning Model (LLM) tools such as ChatGPT:

1. Not copying and pasting text from agency emails, the agency intranet, or government websites into any Artificial Intelligence (AI) Large Learning Model (LLM). Large Learning Models (LLMs) like ChatGPT and Bard are designed to learn from prompts and user queries.
2. Not directly providing Large Learning Models (LLMs) with information from department computer systems like Computer Aided Dispatch (CAD), the Records Management System (RMS), Law Enforcement Information Exchange (LinX), Motorola's CommandCentral, ISOClaims (NICB), Starlight, or any other law enforcement / public safety software.
 - a. Instances have been documented where Large Learning Models (LLMs) have incorporated *sensitive* user-provided information into subsequent responses. User-supplied questions and Artificial Intelligence (AI)-generated answers are **not** secure.
3. Artificial Intelligence (AI) researchers can access user-provided documents and prompts. If sensitive information is transmitted to an AI tool, it becomes part of **their** Large Learning Model (LLM). Others may view it, including Artificial Intelligence (AI) developers at Google and Microsoft.
4. Not using AI tools to analyze and interpret PDF documents like ChatPDF on official government correspondence or court documents such as search and seizure *warrants*, Standard Operating Procedures (SOPs), department policies, or procedures.
5. **Avoid** using AI-generated images in criminal investigations. Facial generators are becoming increasingly accurate, with significant advancements occurring, on

average, every three to five days. There are no established legal policies and procedures to guide law enforcement except within the civil realm.

6. Before using any Artificial Intelligence (AI) tool, review any provided Terms of Service and Privacy Statements.
 - a. Avoid using any Artificial Intelligence (AI) tool that does not make its *Terms of Service* and *Privacy Statements* available for users to read, save, or review the update/publication date.
 - b. Within Terms of Service, Large Learning Models (LLMs) often provide a disclaimer that their information may be offensive or inaccurate. Therefore, it is advised that users independently check the data source for accuracy before using it as an information source.

As the department navigates the era of Large Learning Models (LLMs), harnessing the immense potential for positive advancements is balanced with safeguarding department members and our agency against unintended harm.

The rapid advancement of Artificial Intelligence (AI) Large Learning Model (LLM) tools, including ChatGPT3.5/4, Copilot, Gemini, Art Breeder, Midjourney, and Sudowrite, has captured widespread attention across the internet. Their impact extends across various applications, from natural language processing and translation to content generation and scientific research assistance.

Artificial Intelligence (AI) tools have the potential to streamline processes, enhance decision-making, drive innovation in numerous industries, or disrupt ongoing efforts to keep the public safe. Therefore, it is crucial to approach their use with careful consideration.

While the development of Artificial intelligence (AI) tools is still in its early stages, there have been noteworthy instances where these tools have *negatively* impacted public safety and law enforcement.

Utilizing best practices and caution is the best way to ensure sensitive law enforcement data and information confidentiality.