RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS APRIL 2024

Navigating the Risks and Rewards of AI in Public Entities

by Cindy C. King, Director of Membership Services and Human Resources

AI's fake text, images, and videos are hard to distinguish from the real thing, making AI the ideal tool for digital deceivers.

PERHAPS YOU HEARD OF the CFO who was deceived by deepfake technology and cost his employer $25 million. Artificial Intelligence (AI) was used to mimic the voices and faces of the CFO's executive colleagues in a video meeting. The CFO later said that everyone in the virtual meeting was someone he knew. He recognized their faces, voices, and even the backgrounds of the offices they worked in. At their urging, he proceeded to transfer $25 million worth of corporate funds to various bank accounts. However, those individuals were entirely simulated using deepfake technology.[1]

MMRMA's Risk Management Workshop in Lansing featured *Good and Bad of AI,* a discussion facilitated by Scott Brady of Future Point of View. Brady described today's AI as a "brilliant child who needs a lot of attention and guidance."

During a March 20, 2024 webinar, *Building Your AI Strategy,* Jim Carpp, Chief Digital Officer of consulting firm Rehmann, identified "activities [that] can be generated by AI" such as seeking information, building content, learning your pattern of writing, knowing current events, and other activities.

Weighing risks and rewards

Both organizations and people are trying to understand what AI means to them. MMRMA member public entities may be wondering if AI is a useful tool that could help them deliver constituent services—or a sinister risk to be avoided. As with many complex topics, the answer is somewhere in the middle.

AI has been described as a "brilliant child who needs a lot of attention."

Wikipedia defines AI as "intelligence exhibited by machines, particularly computer systems, as opposed to the natural intelligence of living beings. ...[By] focusing on the automation of intelligent behavior through techniques such as machine learning, AI develops and studies methods and software which enable machines to perceive their environment and take actions to maximize their chances of achieving their goals, with the aim of performing tasks that are typically associated with human intelligence."

Wikipedia lists advanced web search engines, autonomous vehicles, and "superhuman play and analysis in strategy games" as potential applications of AI.[2]

Chatbots and generative AI

ChatGPT is one of many AI tools garnering attention. Launched in late 2022, the chatbot is driven by generative AI technology, which can create text, images, and video. Organizations, including public entities, might use this tool for composing emails, assisting with routine tasks, or composing thought papers.

Nathan Rogers writes on *LinkedIn* about potential uses

continued on page 2

1 https://www.shrm.org/topics-tools/news/technology/deepfake-scams-expose-employers-risks
2 https://en.wikipedia.org/wiki/Artificial_intelligence

Risks and Rewards of AI, continued from page 1

of ChatGPT in local government: [3]

1. Writing a business case.
2. Creating job descriptions.
3. Answering citizen questions.
4. Getting a start on a task such as drafting a policy.
5. Providing advice to members of a city council or township board.

Enhancing safety and service

AI could enhance efficiency in delivering local government services. The City of Detroit is using a $2 million federal grant to pilot AI software to complement existing traffic cameras and establish more than a dozen "smart intersections." The aim is to eventually predict and prevent traffic incidents. AI will capture real-time data and track crashes—or near misses—in those corridors.

Tim Slusser, Chief of Mobility Operations for the city, says the program will "help us define these root causes so we can better aim our mitigation and our strategies to improve road safety." According to Slusser, Detroit consistently ranks among the top metropolitan areas for traffic incidents and road fatalities.

He states: "If there was a near miss that involved a pedestrian walking in the street, AI could help determine:

AI could be used on an ongoing basis to monitor if and when roads and bridges need maintenance or repairs.

Was the light red or green? Was the pedestrian or driver doing something wrong? Was it caused by improper timing of signals? Or maybe the light went out?" [4]

AI might also be used to improve operations in public utilities. For example, it could gather data in water distribution systems to determine peak usage times and help maintain a reliable supply of water. Another potential use of AI is to determine when roads and bridges need maintenance or repairs.

Implications and risks

However, as Scott Brady noted at the Risk Management Workshop, AI can have unanticipated ethical implications such as biases, human skill loss, decision inaccuracy, data corruption, and automation errors.

The first step in managing such risks is to establish an AI policy that clearly defines what data is off-limits for uploading into any AI tool, particularly data that contains sensitive Personally Identifiable Information (PII) such as dates of birth and social security, driver's license, passport, credit card, and bank account numbers. Other prohibited data includes confidential contracts, software source code, and patient medical records. [5]

The challenge is to develop AI policies that balance innovation with accountability.

According to a Bloomberg article, the City of Boston identified three simple guides to foster public trust in a municipality's use of AI: [6]

1. Don't include sensitive or confidential information in prompts.
2. Disclose use of the tool so citizens are aware.
3. Review AI outputs for accuracy and sensitivity.

A strategic approach

Broadly, a sound AI policy will address ethical and professional standards, security, safety, compliance with data and privacy laws, and data integrity. In time, most public entities will use AI for the many benefits it can provide. That said, it's important to recognize the inherent risks and address them via policies, scrupulous practices, and ongoing monitoring of your organization's uses of this emerging and complex technology.

While AI can significantly enhance efficiency and service delivery, as demonstrated in various municipal applications, it also brings challenges such as ethical concerns, the potential for misuse, and the need for robust data protection.

Public entities must navigate these waters carefully, ensuring that AI technologies align with the values and needs of the communities they serve.

3 https://www.linkedin.com/pulse/5-uses-cases-chatgpt-local-government-nathan-rogers/
4 https://www.mlive.com/public-interest/2023/04/detroit-hopes-ai-software-could-help-predict-prevent-traffic-crashes.html
5 https://www.linkedin.com/pulse/growing-risks-sensitive-data-leaks-through-ai-tools-guide-vaducha/
6 https://bloombergcities.jhu.edu/news/cities-are-ramping-make-most-generative-ai

The Importance of Body Worn Cameras in Jail Facilities

by Tom Cremonte, Senior Risk Control Consultant, and Randy Hazel, Risk Control Consultant

Stationary security cameras do not capture audio, leaving interactions between staff and inmates open to interpretation.

BODY WORN CAMERAS HAVE been an important tool in law enforcement for many years. When body worn cameras were first introduced, staff were reluctant to use them, leery of management's intentions and potential public scrutiny of how an officer responded to an incident.

Over time, the impact of body worn cameras on the profession has been immeasurable, providing the public with transparency and accountability in its law enforcement agencies. Body worn cameras have become standard-issue equipment for many agencies. Since they have become so widely used, the absence of body worn camera footage of an incident often raises public suspicions.

Mounted cameras limited

Unlike in law enforcement, use of body worn cameras in jails has not yet become an industry norm. Most jail facilities across Michigan have security camera systems covering large portions of the facility. Security cameras are typically focused on high traffic areas such as intake, observation cells, hallways, housing units, and classification and medical areas.

An increasing number of agencies recognize the importance of body worn cameras within corrections settings. Security cameras are certainly important, but there are issues with relying solely on them to provide adequate coverage in jail facilities.

Use of body worn cameras in jails has not yet become an industry standard.

Many security systems installed in facilities around the state include aging and outdated analog equipment. The concern with older generation camera systems is that quality is often inferior to newer, digital options. Upgraded digital camara systems offer multiple benefits, including a clearer picture, the ability to capture larger areas with fewer cameras, zooming in without sacrificing image clarity, and the ability to record audio as well as video.

Although technology has advanced for security cameras in jails, relying solely on these systems can be problematic because they are stationary and cannot capture every aspect of the jail. Use of body worn cameras becomes crucial in these instances.

Benefits in corrections

When an incident is captured by a facility's security camera system, it omits verbal interactions between staff and inmates. Without audio to support video footage, much of the interaction is open to interpretation.

Body worn camera footage lends a second, more personal view and another angle to that of security cameras. Body cameras also provide coverage in those areas not visible to stationary security cameras. For the most thorough coverage of an incident, it is highly recommended to supplement existing security camera systems with body cameras.

Review incidents to create a plan

If an agency chooses to upgrade their security camera system and/or add body worn cameras, review past incidents in the jail to help pinpoint areas with high incident rates or blind spots.

Such a review will identify which security cameras should be replaced and show which parts of the jail require additional cameras for increased coverage and surveillance. The review should also offer insight into the areas that stationary cameras cannot cover and where the facility would benefit from the addition of body worn cameras.

Develop policies and training

When introducing an upgraded security camera system or body worn cameras into a facility, it is essential to update policies. A security camera policy should outline who is authorized to access stored video, the proper use and monitoring of footage, incident retention, data storage, and an overwrite schedule.

Jails may purchase body worn cameras for all on-duty staff, or only for staff members who are assigned to high traffic areas. The policy should reflect which staff members will be issued a body worn camera, where it should be placed on the uniform, and when it is to be used—such as during cell

continued on page 4

RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

Tech Giants Roll Out New Email Security Standards

By Daniel Bourdeau, Cybersecurity Practice Leader

YOU'RE SIPPING YOUR morning coffee, browsing your emails, and notice something different. The tech trifecta—Google, Microsoft, and Apple—have joined forces to roll out a new email authentication requirement. This isn't just any update; it's like the Avengers tackling the ever-present villains of our online world: phishing and spam.

Here's the scoop: Our digital guardians are implementing stricter standards for email authentication. Think of it as a bouncer at the club door, but for your inbox. This new protocol aims to verify that the emails you receive are actually from who they claim to be and not from an impostor trying to swindle you.

Why does this matter?

Phishing scams have been as common as road construction barrels in Michigan. They're everywhere, they're annoying, and they're dangerous. These scams can lead to significant security breaches, leaking personal and sensitive information faster than a secret in a small town.

With these new measures, Google, Microsoft, and Apple are saying, "Not on our watch." The new standards combat fraudulent emails, make it harder for digital deceivers to reach your inbox, and reduce the chance that you'll accidentally click on a malicious link that promises you millions but delivers malware instead.

Even more exciting is the potential ripple effect this collaboration could have across the tech industry. When these giants move, others follow. They introduce a new standard, encouraging a safer digital environment for all of us. When you open an email, you can be a bit more confident that it's legitimate—unless, of course, it's asking you to wire money to claim your lottery winnings from a country you've never visited.

In a world where our digital and real lives intertwine like spaghetti and meatballs, this move by Google, Microsoft, and Apple is a welcome step toward making the internet a safer place. Hats off to these tech titans for adding another layer of armor in our ongoing battle against cybervillains.

So the next time an email from a supposed prince slips through, take time to update your email settings. If you don't take action now, your agency may find itself isolated on a deserted island, with employees unable to receive important emails they need to do their work.

Body Worn Camera in Jail Facilities, continued from page 3

extraction, inmate transports, inmate interviews, and disturbances. Policies should state who and how body worn cameras will be maintained.

Other policy considerations include events or areas prohibited from recording, a video retention schedule, and a confidentiality statement. Staff using body worn cameras should indicate in their written reports that video is available.

Whenever a new or updated policy and equipment are introduced, it is essential to provide and document related training. Team training on new security camera systems or body worn cameras may include policy review, use and care of the equipment, uploading and saving incident videos, how to review video and how to attach a video to the written report. MMRMA's Membership Services team can provide recommendations in these areas.

Calling all runners, walkers, and hikers: April is time for Run for the Trees: A Happy Little 5K. You pick the pace and the place, run anywhere outdoors between April 22–26, and log your completed run online. Inspired by PBS painter Bob Ross's love of the outdoors, the event has, since 2019, raised enough money to plant more than 2,100 trees in 20 state parks across Michigan.

The *Risk Journal* is edited by Tamara Christie, Communications Manager, and published six times a year for members of Michigan Municipal Risk Management Authority. We welcome your feedback. To comment or suggest story ideas, please contact Tamara at 734 513-0300, 800 243-1324, or tchristie@mmrma.org.