Milwaukee Facial Recognition Technology Use - ERC Meeting - Wed June 18, 2025

Hello, my name is Katie Grillaert and I am a responsible tech and AI governance advisor, and AI systems auditor. On April 17th, I provided public comment to the Fire and Police Commission meeting. I stated that I was against the use of this technology for reasons based on privacy and overreach of government. Due to time limitations, I did not discuss the potential for disparate impact on racialized and marginalized community members, and I expected that many others would give comments on this - and they did, unanimously, emphatically, and compellingly.

Today, I am going to comment from another angle. In the spirit of protect and serve, and with the assumption that we all agree upon the deployment of secure and responsible technology in our community, I will present a few components of how this proposal should be approached, with relevant questions, and a few tools to be used in the process. Each of these questions must be answered clearly, specifically, and thoroughly, risks addressed and mitigations proposed, before the community is informed enough to even consider a "yes" response to this technology.

0. **Agreement**. What is the exact data that the MPD would be trading for the software license? What is the term of the license agreement?

1. **Scope**, **Nature**, **Context**, **Purpose**. This is a technical framework for understanding the system components and how it will be used. From a community perspective, we also need a layman's version that explains the SNCP within the actual community, with roles, responsibilities, and accountability clearly defined and assigned.

2. **Stakeholder engagement**. Spend significant time listening to concerns of stakeholders. Create a committee of diverse perspectives, considering protected demographics as well as education, career, neighborhood, and other relevant identities. This committee gives feedback directly to the Ethics committee.

3. **Ethics committee**. This committee must be composed of people specifically trained in philosophy, ethics, human rights, and AI systems. The ethics committee uses tools such as a **Risk/Impact Assessment**, **Fundamental Rights Impact Assessment** and **Disparate Impact Assessment** to safeguard human rights.

4. **Provider Due Diligence**. The Provider of the system (Biometrica) should provide comprehensive and satisfactory answers to questions including (and not nearly exhaustive): What data was used to train their system? Who owns the data and how is it used when MPD provides input during use of the data? How was the model tested for accuracy, reliability, robustness? How and when is the model tested for drift? How is the model and system secured from cyber threats? What ethical choices were made during the design and development of the system and what ethical and diverse input was used to inform these choices?

5. **Human oversight**. Where is the human-in-the-loop? How are they trained, what are they trained on, and who provides the training? How are they held accountable? What are redress avenues for targets of the system?

6. **Personal Data and Privacy**. What does MPD do with the data? How can they use the data? For how long is it retained? Can it be linked to other personal data, whether publicly or privately obtained? How do people consent to use? How are people notified that they are subject to active system use? How do people know that their data has been collected? How do people know how their data is being used? How does the MPD secure the system from physical and cyber threats? What AI literacy is provided to MPD, who does the training, what does it cover, and how is effectiveness evaluated?

7. **Interpretability and Explainability**. Can we trace the input to the outputs? How can we interrogate the output? What are the variables and features used in the algorithm? Can the system communicate uncertainty or confidence in its outputs?

8. **Monitoring and Incident Response**. Who monitors the system for drift, accuracy, reliability, robustness? What is their background and training for the role, and how are they held accountable? How are incidents monitored and logged? How is this information provided publicly? What are the systems and processes to respond to incidents? What is civilian recourse for incidents?

9. **Decommissioning**. How will it be determined that the system does not meet ethical and/or performance metrics required by the community and ethics committee? What metrics will be used, who decides the metrics, who monitors the metrics? How will satisfactory performance be communicated regularly to the community? When and how will the community be able to give feedback on continued use or change of metrics? How often will fundamental rights and disparate impact be measured? How will the system be fully and transparently decommissioned if it does not meet metrics and maintain community approval?

Heather Hough, chief of staff for MPD, is quoted as saying “"We desire to keep everyone safe and we recognize the very delicate balance between advancements in technology and ensuring we as a department, do not violate the rights of all of those in this diverse community of interest that we serve," but also wanted the public to know that MPD was under no obligation to inform Milwaukee residents it was considering adopting this technology, but decided to bring it forward to hear how the community felt.

While it may not be legally required to inform Milwaukee residents about this technology, it is an ethical imperative, not a favor. In order to avoid violating rights of the community, and responsibly deploying technology, MPD is likewise ethically compelled to transparency and thoroughness in the processes I have outlined above. Thank you.