HB1046 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

FAVORABLE WITH AMENDMENT

Chairman Clippinger, Vice Chair Moon and members of the Judiciary Committee, my name is Owen Larter, I am Director of Public Policy in the Office of Responsible AI at Microsoft, thank you for the opportunity to submit testimony.

Microsoft would like to thank Senator Sydnor and Delegate Moon for their leadership on the issue of how to ensure facial recognition technology is used responsibly. This bill represents an important step forward in giving people protection under the law. Through this bill, Maryland has the opportunity to set itself apart as only the second state in the United States to establish specific guardrails to ensure that the use of facial recognition technology by law enforcement is rights-respecting, transparent, and accountable.

Facial recognition can provide many benefits to society, including helping secure devices and assisting people who are blind or with low vision access more immersive social experiences. In the public safety context, it can be used to help find victims of trafficking, or as part of the criminal investigation process.

However, without clear guardrails that have the force of law, facial recognition technology can also pose potential risks to individuals and society. There are three important types of potential risks around facial recognition technology:

- A risk of bias and unfair performance, including across different demographic groups;
- the potential for new intrusions on people's privacy; and
- possible threats to democratic freedoms and human rights.

Microsoft is clear-eyed about the potential risks that facial recognition can pose if not developed and used responsibly. Since 2018, we have engaged in an expansive program of work to design and enact effective safeguards to help secure its responsible use. This has included the internal adoption and implementation of Facial Recognition Principles[1] and the development of our Face API Transparency Note[2]. The Transparency Note helps customers make informed decisions about how best to responsibly deploy our facial recognition service. It communicates, in understandable language aimed at non-technical audiences, how Face API works and the factors that will affect system accuracy. It also emphasizes the need to think about the whole system during deployment, including the importance of having a human in the loop.

In addition to these safeguards, Microsoft continues to believe that there is an urgent need for regulation. This need is particularly acute in the law enforcement context, given the consequential nature of the decisions that police take.

Microsoft strongly believes that facial recognition should not be deployed by police without specific civil liberties protections and safeguards in relation to transparency and accountability, testing, and human review. Microsoft believes this bill introduces some important safeguards, including:

- **Robust civil liberty protections**, such as restricting the use of facial recognition to establishing probable cause or positive identification in relation to only the most serious crimes, and only in conjunction with other independently obtained evidence. The prohibitions on real-time identification and the use of facial

[1] Microsoft, *Six Principles for Developing and Deploying Facial Recognition Technology*, https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf.
[2] Microsoft AI, *Transparency Note: Azure Cognitive Services: Face API* (2019), https://azure.microsoft.com/mediahandler/files/resourcefiles/transparency-note-azure-cognitive-services-face-api/Face%20API%20Transparency%20Note%20(March%202019).pdf.

recognition on an individual suspected of being a juvenile provide further important protections, as does the prohibition on using the technology on the basis of an individual's engagement in constitutionally protected activity or their race, color, religious beliefs, sexual orientation, gender, disability, national origin or status as being homeless.

- **Transparency and accountability requirements**, such as the need for an agency to adopt a model policy on facial recognition use and a data management policy. It will be important that these policies are developed in a way that ensures police can identify and address risks around a system and keep data secure. The need to complete an annual audit to determine compliance with the law and use policies is also important, as is the restriction of facial recognition searches to high quality images in drivers' license and mugshot databases, which will deliver better quality results and provide transparency around the databases police are searching.

- **Important requirements around human review** of facial recognition output and the training and testing of the reviewer.

We do, however, think the bill can be strengthened, most notably by requiring two types of testing of facial recognition systems. First, the bill should require that vendors offering facial recognition services enable legitimate and reasonable third-party testing of their services. This is critical given the variation in accuracy across vendor offerings[3]. Third party testing is therefore needed to ensure law enforcement can identify and use more accurate systems that can be trusted by the public to perform well, including across different demographic groups.

Second, the bill should require agencies deploying facial recognition to subject those systems to operational testing prior to deployment in the environment in which they will be used. This is because environmental factors like lighting and camera positioning have a material impact on accuracy. Requiring that systems are tested and that any gaps in performance are addressed is therefore vital in ensuring police are using technology in a way that builds public trust.

Microsoft believes this bill represents important progress. We recognize that it is the product of an ongoing conversation between lawmakers, civil society, and law enforcement which we have welcomed the opportunity to contribute to. We look forward to continuing to contribute to this effort, now and in the future, with a view to building out safeguards for the responsible use of facial recognition that are robust and durable over the long term.

[3] National Institute of Standards & Technology, Face Recognition Vendor Test (FRVT) (2022) 5, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.