ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Testimony of:

Ashley Johnson and Juan Londoño
Senior Policy Manager and Policy Analyst
Information Technology and Innovation Foundation

Before the:

Baltimore City Council Committee on Health, Environment, and Technology

Hearing on:

"Facial Recognition Technology"

November 14, 2023
Du Burns Chamber, 4th Floor, Baltimore City Hall
Baltimore, MD

Chairwoman McCray and members of the committee, thank you for the opportunity to appear before you to discuss the potential need for Baltimore to regulate the use of facial recognition technology.

My colleague and I are here representing the Information Technology and Innovation Foundation (ITIF). ITIF is a nonprofit, nonpartisan think tank whose mission is to formulate and promote public policies to advance technological innovation and productivity.

In my testimony today, I would like to discuss the benefits and applications of facial recognition technology and the importance of maximizing these benefits while minimizing any potential risks.

Facial recognition technology compares images of faces in one of two different ways. The first type of comparison is known as a one-to-many or identification search, in which the technology searches a database of faces to find potential matches to a particular face. The second type of comparison is known as a one-to-one or verification search, in which the technology compares two faces to determine the similarity between them.[1] Facial recognition technology has rapidly improved in recent years and provides numerous benefits to society.

First, facial recognition has increased public safety. Facial recognition technology has many applications for law enforcement, including locating missing persons, detecting fraudulent activity, solving cold cases, and identifying witnesses, suspects, and other persons of interest. Facial recognition technology can complete these searches in a fraction of the time it would take humans, saving time and taxpayer dollars. In 2018, authorities identified a suspect in the Capital Gazette shooting at a newspaper stand in Annapolis after the suspect had damaged his fingertips to prevent identification and refused to give his name during interrogations.[2]

Second, facial recognition has increased convenience for consumers. This includes streamlining security check-in processes, providing customers with a more personalized experience, and enabling customers to make purchases with a facial scan. This year, the Baltimore-Washington International Airport gained 36 self-service credential authentication technology (CAT) units that use facial recognition to compare an individual's face to the image on their identification, streamlining airport security.[3]

As another example, the real estate company Keller Williams hosted its annual Spring Masterminds event in 2018 at the Gaylords National Resort and Convention Center in National Harbor and gave attendees the option of providing their picture to opt-in for facial recognition to check-in to the event for the first time. Of the 1,360 registered attendees, nearly half opted in to facial recognition and received a badge with a personalized agenda for the event.[4]

Finally, facial recognition has increased security for businesses. Customers can verify their online purchases with their credit card companies by taking selfies, banks can verify customers' identities online and at ATMs using facial recognition, and organizations of all kinds can use facial recognition technology to ensure only authorized individuals have access to restricted areas.

These are only a handful of examples of how facial recognition technology could benefit society. And yet, much of the conversation surrounding new technologies inevitably focuses on the potential risks and downplays or dismisses the potential benefits. This cycle of panic slows the pace of innovation, leading to

missed opportunities that, in the case of facial recognition technology, would have implications not just for convenience but for public safety and security.[5]

It is the job of policymakers to consider the overall impact of new technologies, both positive and negative. In the case of facial recognition technology, there are many clearly beneficial government and commercial uses. Moreover, a combination of existing privacy laws, industry best practices, and government oversight can effectively manage the risks from the technology. Therefore, policymakers can strike a balance with regulation that maximizes the benefits of facial recognition technology while minimizing its risks.

Above all, I commend the City of Baltimore for stepping back from rules that would severely restrict or ban facial recognition technology. Policymakers should recognize that creating a patchwork of laws creates barriers to innovation that hurt both businesses and consumers, and therefore avoid enacting regulations for technology at the local level that create conflicting or duplicative rules with state and federal policies. It is much more appropriate for policymakers to focus on regulating the use of facial recognition technology by city agencies as the amended bill proposes.

Thank you for your consideration.

Ashley Johnson
Senior Policy Manager

Juan Londoño
Policy Analyst

REFERENCES

1. "ITIF Technology Explainer: What Is Facial Recognition?", April 8, 2020, ITIF, https://itif.org/publications/2020/04/08/itif-technology-explainer-what-facial-recognition/.
2. John Bowden, "Authorities identified Maryland shooting suspect using facial recognition software," *The Hill*, June 28, 2018, https://thehill.com/policy/technology/394751-authorities-ided-maryland-shooting-suspect-using-facial-recognition/.
3. "TSA at BWI Airport gets new credential authentication technology to improve checkpoint screening capabilities," Transportation Security Administration, April 26, 2023, https://www.tsa.gov/news/press/releases/2023/04/26/tsa-bwi-airport-gets-new-credential-authentication-technology.
4. Danny Stevens, "CASE STUDY: Face recognition check-in for Keller Williams. Objectives, implementation and results," fielddrive, June 21, 2018, https://fielddrive.com/blog/2018/6/21/case-study-facial-recognition-check-in-for-keller-williams-objectives-implementation-and-results.
5. Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies" (ITIF, September 2015), https://www2.itif.org/2015-privacy-panic.pdf.