RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 024 – 10 February 2021

Facial Recognition: More Peril than Promise?

By Manoj Harjani

SYNOPSIS

The use of facial recognition to identify perpetrators of the US Capitol riot comes at a time of burgeoning debate about when and how such technology should be used, and by whom. In the Singapore context, we should anticipate greater calls for accountability and measures to strengthen public trust as facial recognition is deployed within Smart Nation initiatives.

COMMENTARY

FOLLOWING THE events that transpired at the US Capitol on 6 January 2021, American law enforcement agencies have turned to facial recognition technology to identify perpetrators and bring them to justice.

Techno-optimists bullish about the potential of artificial intelligence (AI) to transform daily life will see such usage of facial recognition technology as yet another example of AI's promise. However, it comes at a time of burgeoning debate in the United States and elsewhere on when and how facial recognition technology should be deployed, and by whom.

Exposed: The Darker Side of Facial Recognition

Facial recognition was not the only AI-powered technology brought under the spotlight following the US Capitol riot. The White House had to debunk a social media post claiming that video footage of President Trump disavowing the rioters was a deepfake.

As AI luminary Andrew Ng has astutely observed, the primary peril from AI is not from a rogue superintelligence, but from how humans use AI. This further underscores the need for appropriate governance of facial recognition technology – and AI more

generally – at a time when it is tempting to deprioritise such endeavours given the many challenges demanding policymakers' attention.

The past few years have seen the darker side of facial recognition technology exposed as part of a broader reconsideration to develop and deploy AI ethically and in the public interest.

Extensive media reporting in 2019 and 2020 shed light on collaborations between China's tech giants and their government to deploy facial recognition systems specifically targeting the Uighur minority. In the US, the George Floyd protests against police brutality that began in mid-2020 prompted a backlash against surveillance driven by facial recognition technology.

Nevertheless, there has been little effective regulation governing the development, sale and use of facial recognition technology, which continues to attract considerable interest from governments and law enforcement agencies globally. In a 2019 report, the Carnegie Endowment for International Peace found that at least 75 countries were actively using facial recognition technology.

Irresistible Crutch for Law Enforcement

American law enforcement agencies were quick to employ facial recognition technology following the US Capitol riot. US-based facial recognition startup Clearview AI reported a 26 percent increase in searches by law enforcement agencies on January 7, 2021 over its usual weekday search volume.

This is significant because Clearview claims that more than 2,400 law enforcement agencies across the US use its software – this despite the startup coming under fire for its data scraping practices.

If Clearview's claims are to be believed, the recent public backlash against facial recognition technology – supported by a growing body of research documenting the propensity for gender and ethnic bias – appears to have largely been ignored by American law enforcement agencies.

With only scattered city and state-level regulations at present, there are few incentives for law enforcement agencies to give up using facial recognition technology. Furthermore, tech giants such as Amazon, IBM and Microsoft have already lined up lobbying resources to shape any future federal regulations proposed by the Biden administration and Democrat-controlled Congress.

Smart City Solutions: Pros & Cons

Of potentially greater long-term concern, however, is the export of facial recognition and other surveillance technologies as part of smart city solutions, particularly by Chinese tech companies. A 2020 report by the Brookings Institution highlighted that at least 80 countries had adopted Chinese surveillance and public security technology platforms since 2008.

This bundling of facial recognition and other surveillance technologies into broader

smart city solutions conveniently sidesteps the need to seek societal consent for their adoption. This is generally the case as smart city initiatives are often presented as essential for future economic growth and improved public service delivery.

Furthermore, by treating the deployment of these technologies as inevitable, little or no consideration is given to legitimate concerns regarding gender and ethnic bias. This poses a significant obstacle to implementing ethical principles and frameworks governing the development, sale and use of facial recognition technology and AI more generally.

Facial Recognition in Singapore: Accountability & Public Trust

The use of facial recognition technology in Singapore predates the government's Smart Nation effort, with the Immigration and Checkpoints Authority deploying it at Singapore's borders since 2012.

However, no data is publicly available on the efficacy of this facial recognition system, or whether it has been subject to an audit to determine its susceptibility to gender and ethnic bias. While Singapore has developed a Model AI Governance Framework, this has primarily been pitched as a guide for the private sector.

At the same time, concerns are likely to grow as the government rolls out facial recognition in other areas of public service delivery as part of the Smart Nation push. These include "crowd analytics" via "smart lamp posts" and "face verification" to access government digital services via SingPass.

Calls for the Singapore government to account for its development and deployment of facial recognition technology – and AI more generally – are likely to follow as public awareness matures.

While the government is well-placed to address these concerns, it needs to develop a direct understanding of the public's perspectives and attitudes towards facial recognition and other AI-powered technologies. Engagement through surveys can help in this regard, and results can guide the pace and extent of implementation. Such engagement should be bolstered by public communication efforts.

Building up public trust in facial recognition technology will undoubtedly be a long-term effort. For a start – and to signal openness – the government could apply the Model AI Governance Framework to its own systems and audit them for compliance. Over time, this can be codified into formalised legal protections and mechanisms for seeking redress that apply to both the private and public sectors.

Manoj Harjani is a Research Fellow with the Future Issues and Technology research cluster, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.