Source: *The Straits Times,* pB1
Date: 23 September 2024

Go beyond laws to keep AI from tainting elections

People voting during the 2020 General Election. The proposed Elections (Integrity of Online Advertising) (Amendment) Bill seeks to strike a balance between protecting election integrity and allowing for innovation and freedom of expression in a rapidly evolving campaigning landscape. It is timely with the impending general election in Singapore, which must be held before November 2025, say the writers.
ST FILE PHOTO

AI presents novel challenges to the integrity of elections. How can we strike the right balance to help both candidates and voters?

Carol Soon and Samantha Quek

On Sept 9, a Bill was tabled in the Singapore Parliament to counter digitally manipulated content that may crop up during elections. It will apply to content that misrepresents or misportrays candidates.

The proposed Bill is timely with the impending general election in Singapore, which must be held before November 2025. However, is it sufficient and what more should be done to protect elections in Singapore?

THE GOOD AND THE BAD

Artificial intelligence (AI) technologies can bring a host of benefits to election candidates, voters, fact-checkers and the media. For example, they can make the political campaigning process more efficient, especially when they are used to create campaign speeches, marketing e-mails and write fund-raising texts. AI tools can also be used to perform operational tasks like scheduling and budgeting. In so doing, they free up human labour for more high-touch campaigning activities.

AI tools can also help voters know the candidates better when they are used to reproduce election-related information in native languages. This is especially true for voters from linguistically diverse countries. In addition, AI tools such as Deep Media and Intel's FakeCatcher can help journalists and fact-checkers detect AI-generated and AI-manipulated election-related information, and debunk misinformation quickly.

However, generative AI also poses significant threats to elections. The fabrication of information – AI hallucinations – exacerbates the problem of misinformation.

Second, malicious actors can now produce and disseminate disinformation at scale due to the low cost and ease of use of generative AI tools. The AI-generated robocall message imitating US President Joe Biden reached thousands of voters within two days before the New Hampshire presidential primary. It cost only US$150 (S$194) to produce.

In July, a deepfake video in US Vice-President Kamala Harris' voice – saying she "did not know the first thing about running the country" – went viral. The original poster had claimed it was parody, but tycoon Elon Musk reposted the content without the necessary disclosure. The video was watched more than 128 million times.

During the Indonesian election held earlier in 2024, a three-minute deepfake of late Indonesian president Suharto gained more than 4.7 million views on social media platform X. There was concern over how it would influence public support for the Golkar party.

ENHANCING GUARD RAILS

The proposed Elections (Integrity of Online Advertising) (Amendment) Bill seeks to strike a balance between protecting election integrity and allowing for innovation and freedom of expression in a rapidly evolving campaigning landscape.

The proposed Bill makes it a criminal offence to publish, republish, share or repost digitally manipulated content that depicts candidates saying or doing something they did not say or do. This applies to content produced using AI and non-AI techniques (for example, Photoshop, dubbing and splicing).

The Returning Officer will have the authority to issue corrective directions to individuals, social media services and internet access service providers, or disable access by Singapore users to such content from the issuance

CONTINUED ON PAGE B2

Source: *The Straits Times,* pB2
Date: 23 September 2024

Labelling content can sensitise the public to capabilities of AI tech

FROM B1

of the Writ of Election to the close of polling. Candidates can also request for the Returning Officer to review content that has misrepresented them.

Regulation of digitally manipulated content is not new. Other countries like South Korea and Brazil and some states in the United States have enacted laws to regulate the use of deepfakes or are in the process of doing so. The proposed Bill is surgical in its terms of the "what" (digital manipulation that will be allowed and prohibited), "when" (between the issuance of the Writ of Election and end of Polling Day), and "whom" (providing recourse for candidates).

We feel, however, that especially during a high-stakes period, the proposed provisions could be expanded to increase the transparency of content. In an Institute of Policy Studies working paper, we presented how some governments and technology companies are adopting measures to indicate the origins of the content.

The Brazilian courts have approved resolutions that regulate the use of AI during election campaigns. For example, they require content producers to label AI-generated and AI-manipulated content. In the US state Arizona, people are prohibited from sponsoring, creating and distributing deceptive deepfakes within 90 days of an election, unless there is clear disclosure that the content is generated by AI.

In its community guidelines, tech company TikTok stipulates that users have to label completely AI-generated content or significantly edited media that shows realistic-appearing scenes or people. Such labelling is not required for edits like minor retouching, changing background objects or using TikTok effects or filters.

Apart from flagging deception, labelling content can sensitise the public to the capabilities of AI technologies and make them more digitally aware.

Singapore, meanwhile, is playing the long game on this score. It is building collaborations with diverse stakeholders. For instance, the Sunlight Alliance for Action that was facilitated by the Government roped in researchers, the private sector and civil society to help develop recommendations to combat online harms.

Apart from the proposed Bill, the Ministry of Digital Development and Information said it will introduce a new code of practice to tackle digitally manipulated content beyond elections.

The proposed Bill is surgical in its terms of the "what" (digital manipulation that will be allowed and prohibited), "when" (between the issuance of the Writ of Election and end of Polling Day), and "whom" (providing recourse for candidates). We feel, however, that especially during a high-stakes period, the proposed provisions could be expanded to increase the transparency of content.

The Government has used codes of practice to govern the online space – such as in the domain of online safety and under the Protection from Online Falsehoods and Manipulation Act.

What should the new code of practice establish that has not been addressed by previous codes?

For one thing, the code should establish requirements for transparency and disclosure (for example, declaration of synthetic media content) to help users discern authentic and manipulated content.

It should also establish that tech companies have a duty of care to users and should allocate resources to public education, specifically in promoting greater awareness of the deceptive uses of synthetic media.

Third, the code should establish that tech firms have an obligation to engage researchers to develop evidence-based solutions.

According to the Global Risk Report 2024 by the World Economic Forum, the challenge of mis- and disinformation is ranked the leading global short-term risk (within the next two years), ahead of extreme weather. Safeguarding democratic participation and elections integrity requires agile governance and collaboration.

• Carol Soon is principal research fellow at the Institute of Policy Studies and adjunct principal scientist at the Centre for Advanced Technologies in Online Safety. Samantha Quek is a research assistant at the same institute. They are authors of IPS Working Papers on how to protect elections from threats posed by AI.